IP-COM

User Guide

AP355

1200M 11ac Ceiling Access Point

Copyright Statement

©2016 IP-COM Networks Co., Ltd. All rights reserved.

IP-COM is the registered trademark of IP-COM Networks Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to IP-COM Networks Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of IP-COM Networks Co., Ltd.

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM! Before using your device, please read this guide carefully.

Conventions

If not specifically indicated, “AP”, “this device” or “this product” mentioned in this User Guide stands for AP355V2.0.

As this AP supports both 2.4G and 5G, we will take 2.4G as an illustration throughout this guide.

Typographical conventions in this User Guide:

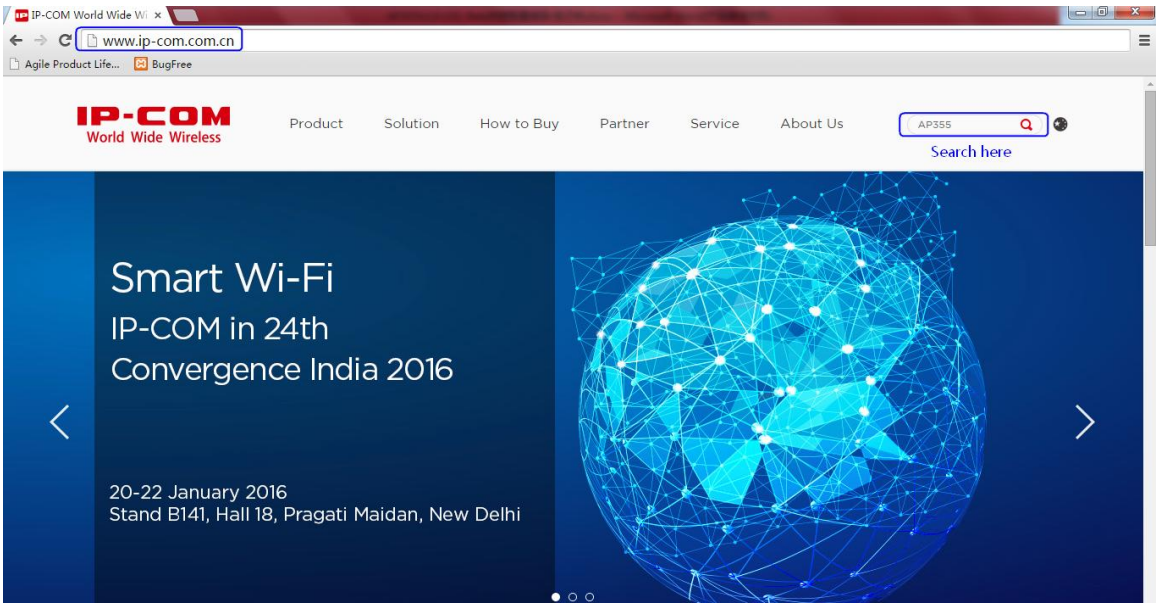
Item	Presentation	Example
Button	Bold	“Click the Save button” can be simplified as “Click **Save**”.
Menu	Bold	“The menu Basic” can be simplified as **Basic**.
Continuous Steps	>	Click **Wireless > Basic**

Symbols in this User Guide:

Item	Meaning
Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
Tip	This format is used to highlight a procedure that will save time or resources.

How to Obtain Latest Product Info

As AP355V2.0 can also be managed by IP-COM access controller AC2000, you can also view the User Guide of AC2000. For latest product information, visit IP-COM official website http://www.ip-com.com.cn and input the corresponding product model in the search bar.



Technical Support

Tel: (86755) 2765 3089

Email: info@ip-com.com.cn

Website: http://www.ip-com.com.cn

Contents

Copyright Statement ..... **i**

Disclaimer ..... **i**

Preface ..... **ii**

Conventions ii

How to Obtain Latest Product Info iii

Technical Support iii

Contents ..... **iv**

1 Product Overview **1**

1.1 Overview 2

1.2 Package Contents 2

1.3 Appearance 2

1.3.1 LEDs, interface & button 2

1.3.2 Label 4

2 Device Management **5**

2.1 Network Tolopogy 6

2.2 Management Method 8

2.3 Web Login 9

2.4 Web Logout 10

2.5 Web Layout 11

2.6 Commonly Used Buttons 11

3 More Features **12**

3.1 Status 13

3.1.1 System Status 13

3.1.2 Wireless Status 13

3.1.3 Traffic Statistics 14

3.1.4 Wireless Clients 15
3.2 Quick Setup 15
3.2.1 AP Mode 15
3.2.2 AP Client Mode 17
3.3 Network 19
3.3.1 LAN Setup 19
3.3.2 DHCP Server 22
3.4 Wireless 24
3.4.1 SSID Setup 24
3.4.2 Radio 32
3.4.3 Radio Optimizing 34
3.4.4 Frequency Analysis 36
3.4.5 WMM Setup 38
3.4.6 Access Control 40
3.4.7 Advanced 43
3.4.8 QVLAN 44
3.5 Firewall 48
3.5.1 URL Filter 48
3.5.2 App Filter 51
3.5.3 Traffic Control 51
3.6 SNMP 53
3.7 Deployment 53
3.8 Tools 56
3.8.1 Maintenance 56
3.8.2 Time & Date 57
3.8.3 Logs 60
3.8.4 Configuration 62
3.8.5 User Name & Password 65
3.8.6 Diagnostics 65

3.8.7 Reboot 65
3.8.8 LED 68
3.8.9 Uplink Detection 68
Appendix 70
A FAQs 71
B Configure PC 72
Windows 8 72
Windows 7 73
Windows XP 75
C Default Settings 77
D Safety and Emission Statement 81

1

Product Overview

Overview

Package Contents

Appearance

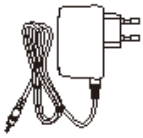
1.1 Overview

IP-COM AP355, the high-density ceiling access point, is an enterprise-grade, high performance Gigabit Wi-Fi access point, prepared for ultra-high density environments. Through the 802.11ac WiFi technology and enhanced transmitted power and receive sensitivity, it can increase WiFi coverage, improve access density and operation stability. You can power on this AP either with the included power adapter or with an IEEE 802.3at-compliant PoE device. Under the management and control of the IP-COM series AC, it supports advanced features like access control, load balancing, seamless roaming, multiple authentication modes and so on. It is an ideal choice for medium-sized enterprise offices, conference halls, multimedia classroom WLAN Deployment.

1.2 Package Contents

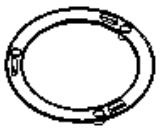
Unpack the package and verify that the following items are included:

Wireless Access Point * 1

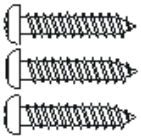


Power Adapter * 1
(12V 1.5A)

Ethernet Cable * 1



Bracket * 1



Screws * 3

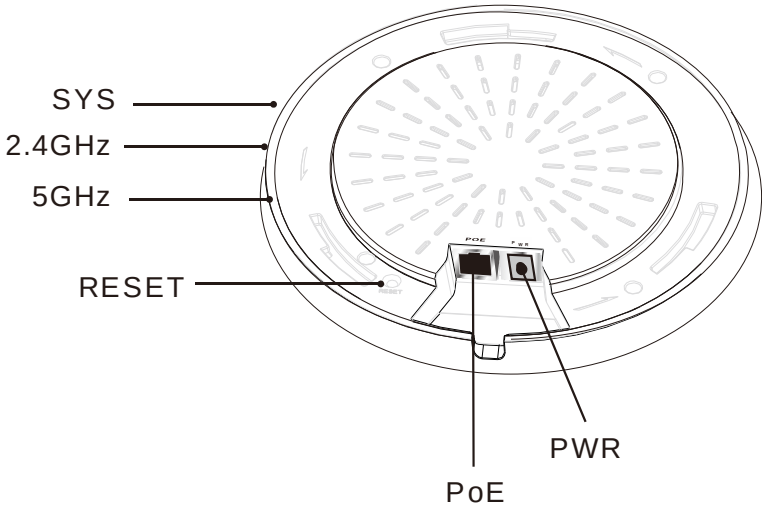
Expansion Bolts * 3

Install Guide * 1

If any item is missing, incorrect or damaged, please contact our reseller with the original package for replacement.

1.3 Appearance

1.3.1 LEDs, interface & button



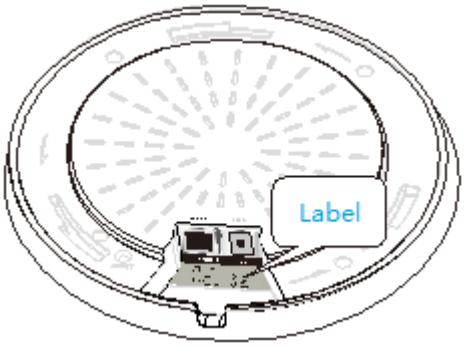
LEDs	Description
SYS	The system/AC LED. When the AP is not managed by an AC (access controller), it displays green. When the AP is managed by an AC successfully, it displays orange. ➢ Solid green: The AP is powered on. ➢ Blinking green: The AP works properly. ➢ Blinking orange: The AP has been managed by an AC. You need to log in to the Web UI of the AC to view the AP's login IP address. ➢ Off: The AP is not powered on, malfunctions occur or LEDs are disabled manually.
2.4GHz	➢ Solid: 2.4G WiFi is enabled. ➢ Blinking: 2.4G wireless data is being transmitted. ➢ Off: 2.4G WiFi is disabled or LEDs are disabled manually.
5GHz	➢ Solid: 5G WiFi is enabled. ➢ Blinking: 5G wireless data is being transmitted. ➢ Off: 5G WiFi is disabled or LEDs are disabled manually.

Interface & Button	Description
RESET	Pressing it for over 7 seconds restores the device to its factory defaults.
PoE	LAN/PoE (802.3at) port. You can connect it to a computer, or an IEEE 802.3at-compliant PoE switch, etc.

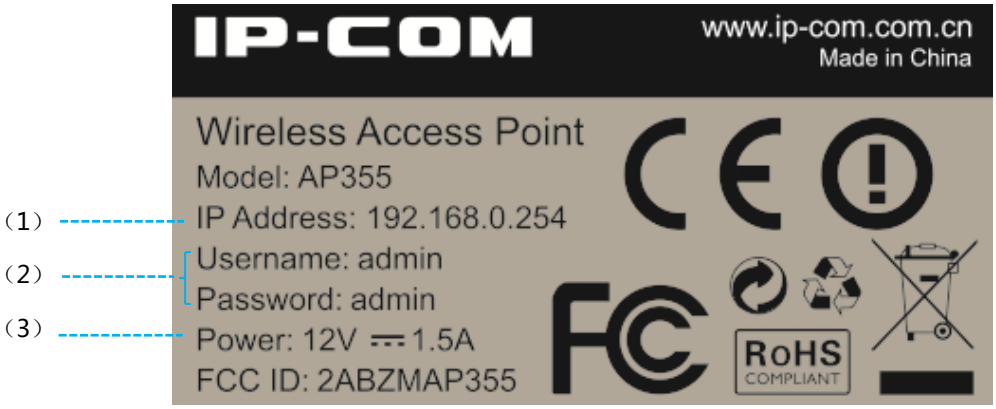
PWR	Used for connecting to the included power adapter for power supply.

1.3.2 Label

The label is attached on the bottom of the device as shown below:



General descriptions of the label:



(1) Default login IP address of the AP. When the AP is not managed by an AC (access controller), you can use this IP address to log in to the web UI of the AP.

(2) Default login user name and password of the AP Web UI.

(3) Power input of the AP. You can use the included power adapter to power on the AP.

2

Device Management

Network Topology

Management Method

Web Login

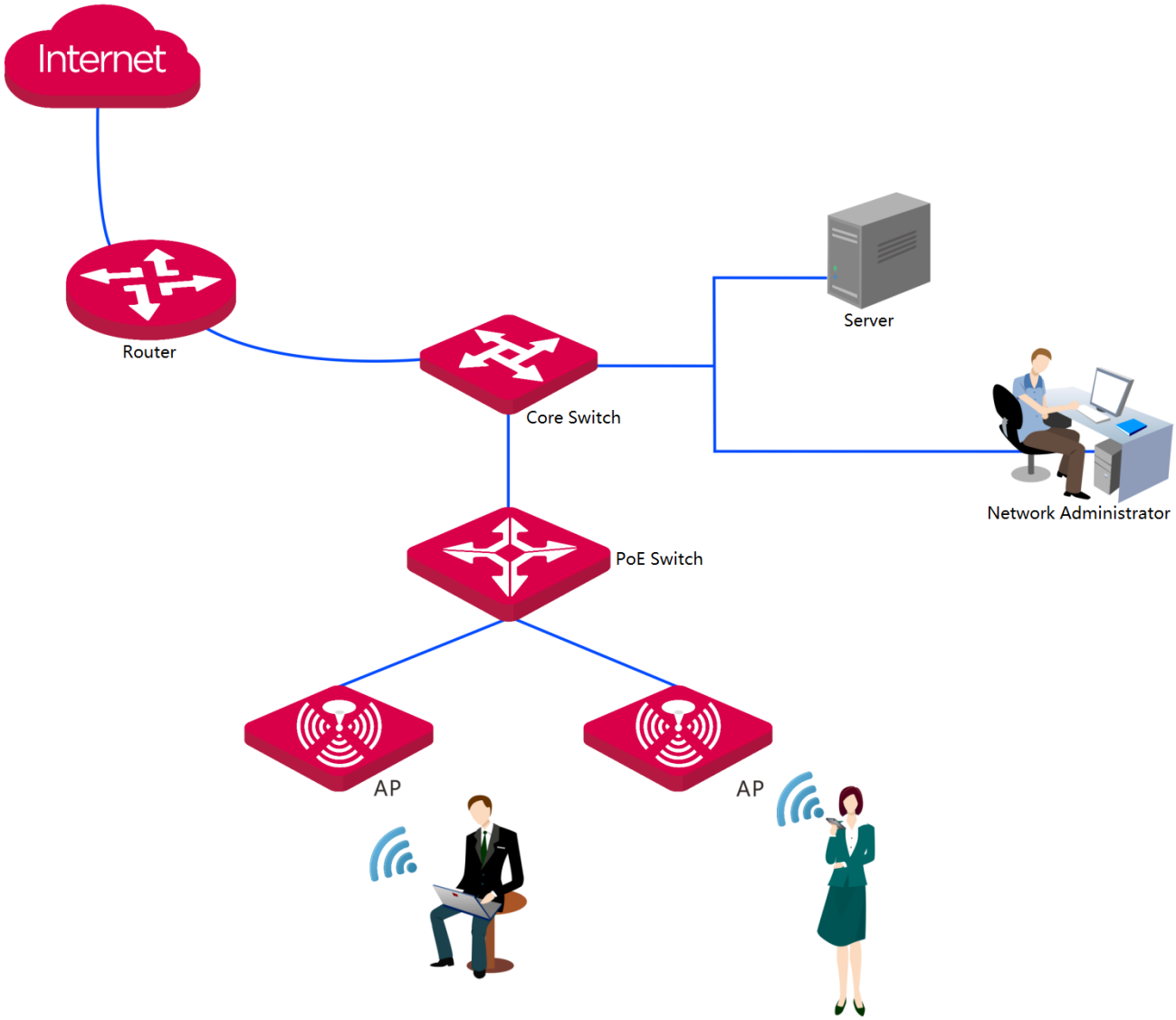
Web Logout

Web Layout

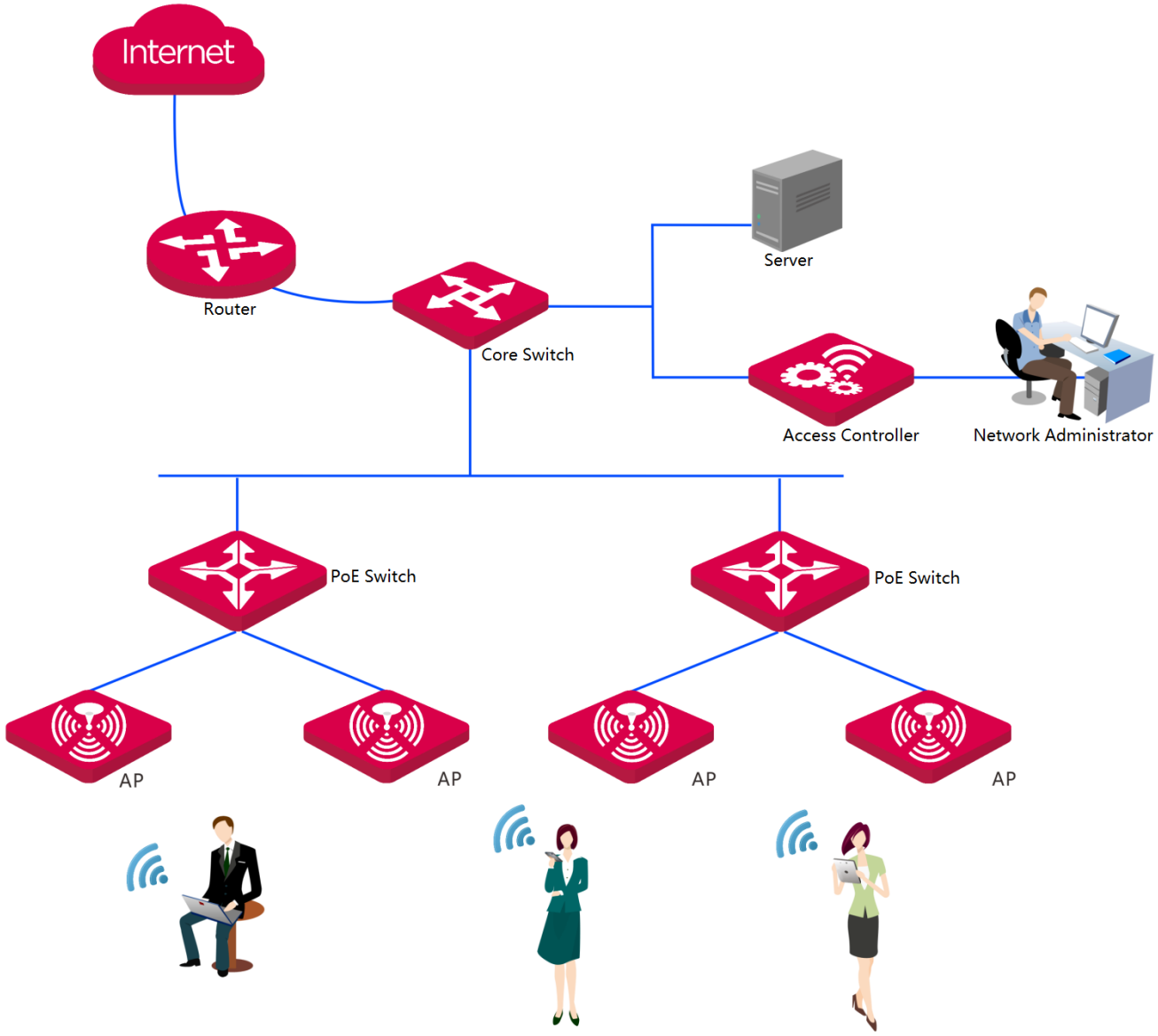
Commonly Used Buttons

2.1 Network Tolopogy

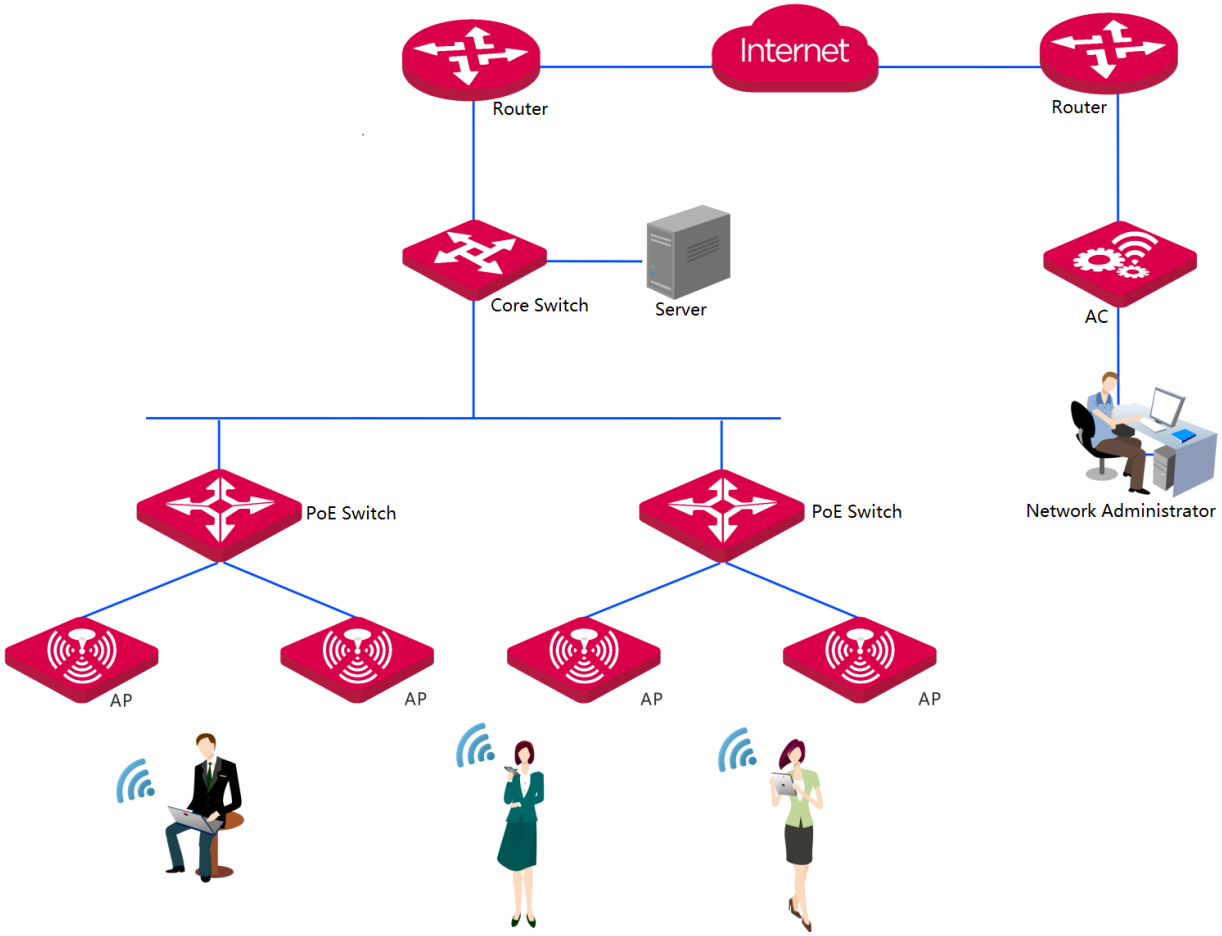
For small-scale networks, you can deploy your network as shown below. In this case, you can manage the AP via its own Web UI.



For centralized, large-scale networks, it is complicated for you to manage all APs independently in your network. In this case, you can deploy an access controller (like AC2000) to manage all your APs (APs work in Local mode) centrally.



When many APs are scattered here and there, it is suggested to set these APs in **Cloud** mode, so that the AC (in cloud mode) from the Internet side can centrally manage these scattered cloud APs.



2.2 Management Method

You can manage this AP either via its own Web UI or via the IP-COM access controller AC2000.

When the AP has been connected to an IP-COM access controller AC2000, it will be managed by the access controller and obtain its IP address info from the access controller. In this case, you can log in to the Web UI of the access controller to manage the AP.

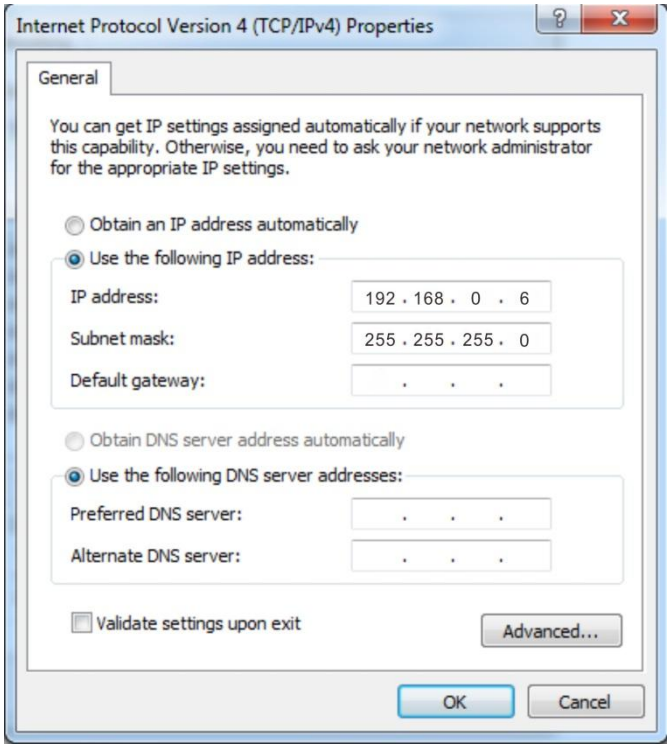
You can visit IP-COM official website http://www.ip-com.com.cn to download User Guide of the corresponding access controller.

In this User Guide, we only instruct you how to manage the AP via its own Web UI.

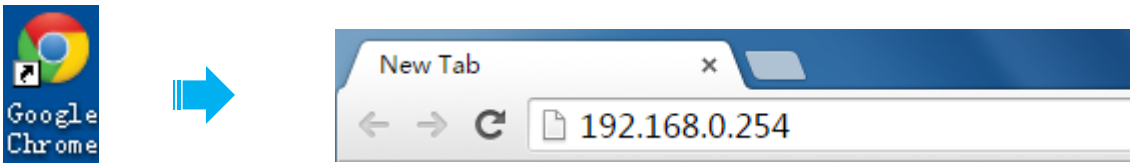
2.3 Web Login

Connect the management PC to the switch which the AP is connecting to and then follow steps below:

1. Set your management PC's IP to a static IP address within the following range: 192.168.0.X (2~253) and a subnet mask of 255.255.255.0.



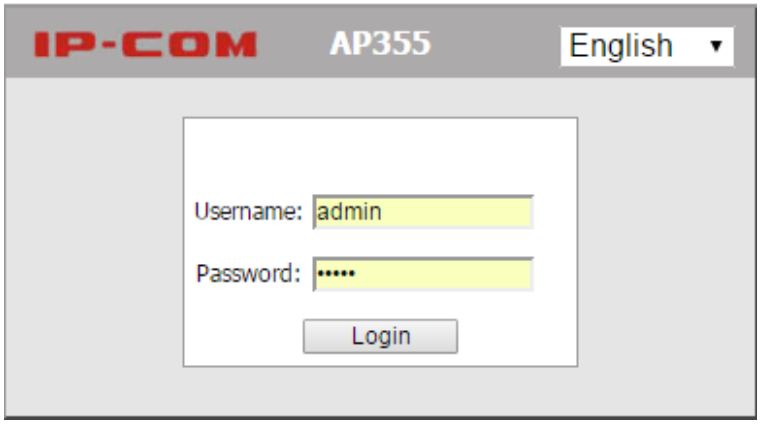
2. Launch a web browser, say "Google", enter 192.168.0.254 in the address bar, and then press **Enter**.



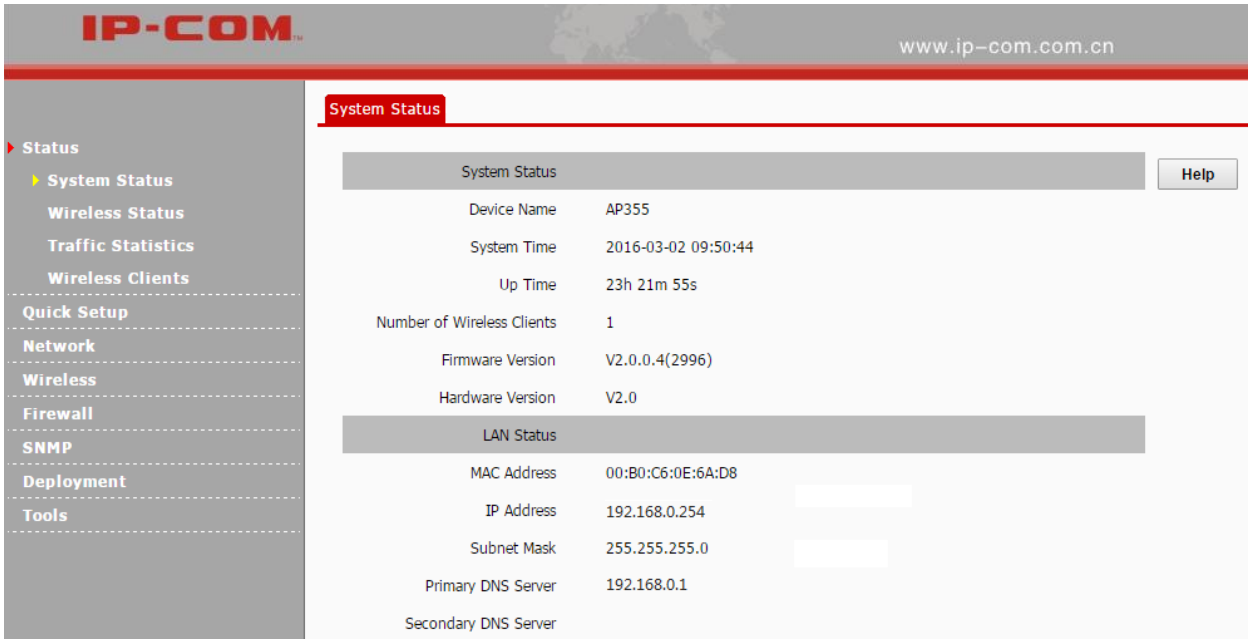
3. Then you'll be prompted to enter the default login username and password (**admin** for both). Click **Login**.

Tip

If the following page does not appear, see FAQ 1.



4. Then you'll be directed to the web UI of the AP successfully. For more settings, see 3 More Features.

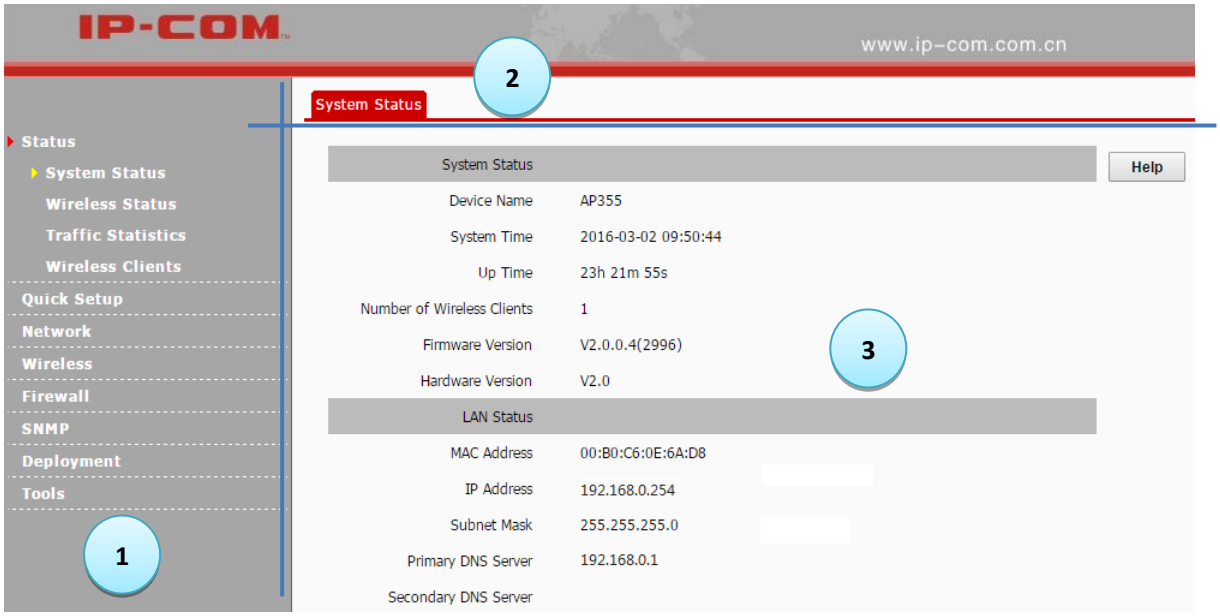


2.4 Web Logout

You will be automatically logged out of the web UI after a period of inactivity. You can set the length of the inactive period, that is to say, the web login timeout is configurable. By default, it is 5 minutes. When it logs out, your current settings won't be saved automatically. Thus, it is suggested to save your current settings before web logout.

2.5 Web Layout

Three parts are included on the web page: primary/secondary navigation, three-stage navigation and the configuration/display section.



ID	Name	Description
1	Primary/Secondary Navigation	Feature menus of the AP. It is very convenient for you to choose feature menus.
2	Three-stage Navigation	
3	Configuration/Display Section	You can configure or view your settings here.

2.6 Commonly Used Buttons

Brief introduction for commonly used buttons:

Button	Description
Refresh	Click it to update info on the current page.
Save	Click it to save and apply your current configurations.
Restore	Click it to cancel current settings that you haven't saved and restore to previous configurations.
Help	Click it to view the help info for the corresponding page.

3

More Features

Status

Quick Setup

Network

Wireless

Firewall

SNMP

Deployment

Tools

3.1 Status

This section gives you an overview of device status and basic information. The following parts are included:

System Status: Display the AP's current system status and LAN information.

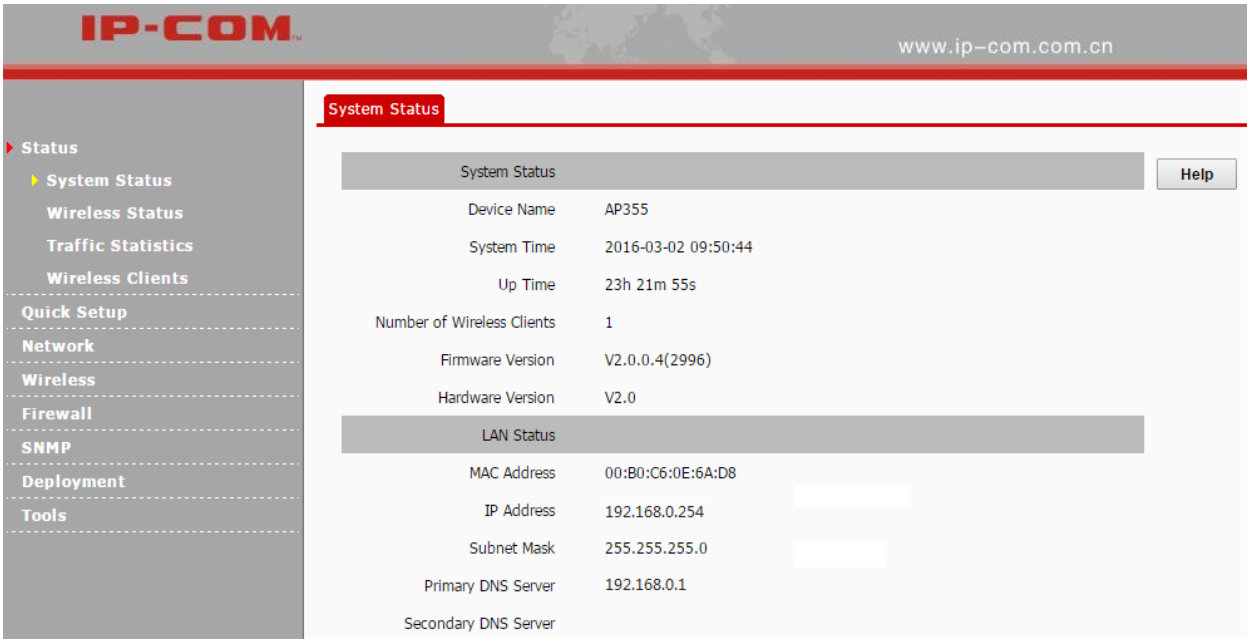
Wireless Status: Display connected devices' radio status and SSID status information.

Traffic Statistics: Display traffic statistics of all SSIDs both at 2.4GHz and 5GHz.

Wireless Clients: Display information of connected devices.

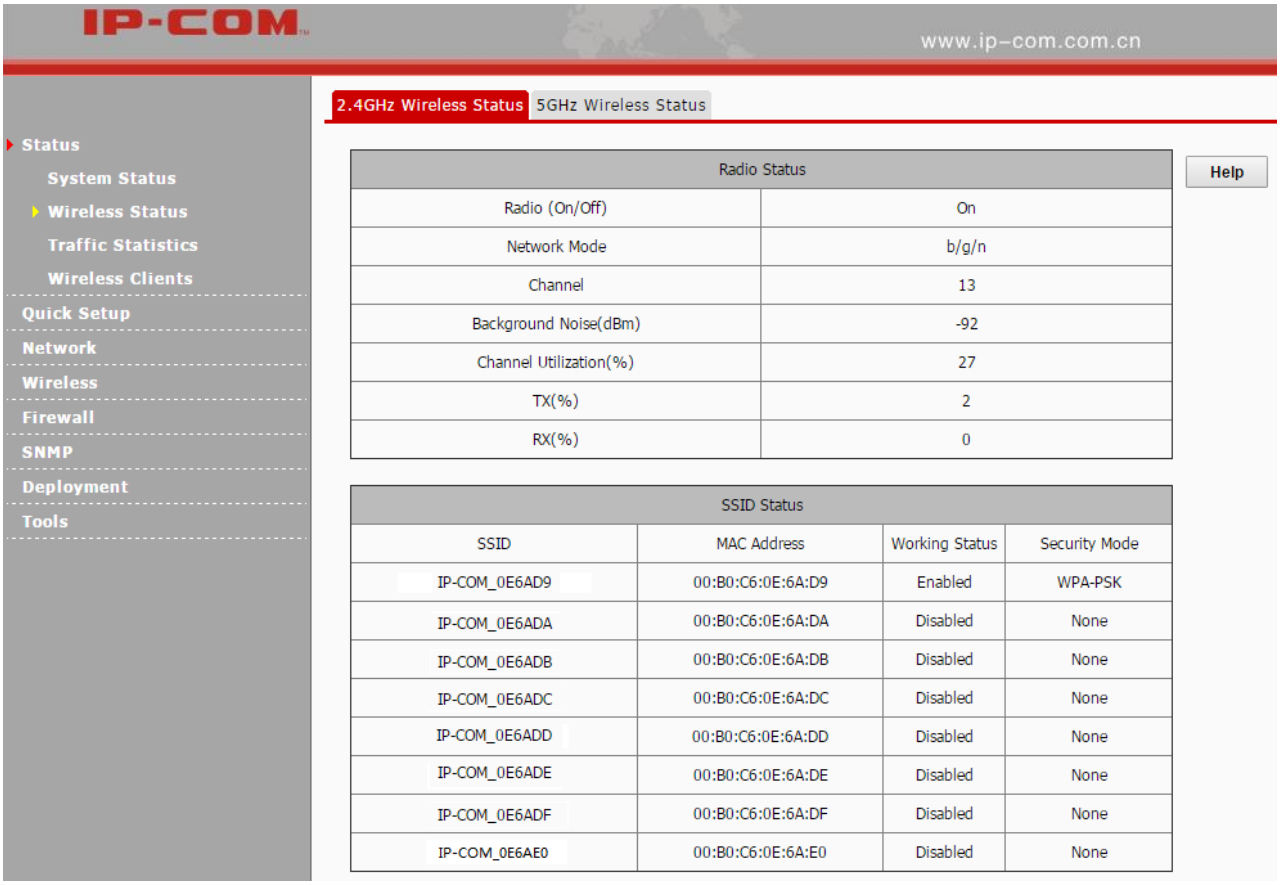
3.1.1 System Status

This page displays system status information and LAN information of this AP, including device name, system time, up time, number of wireless clients, firmware version, hardware version, MAC address, IP address, etc.



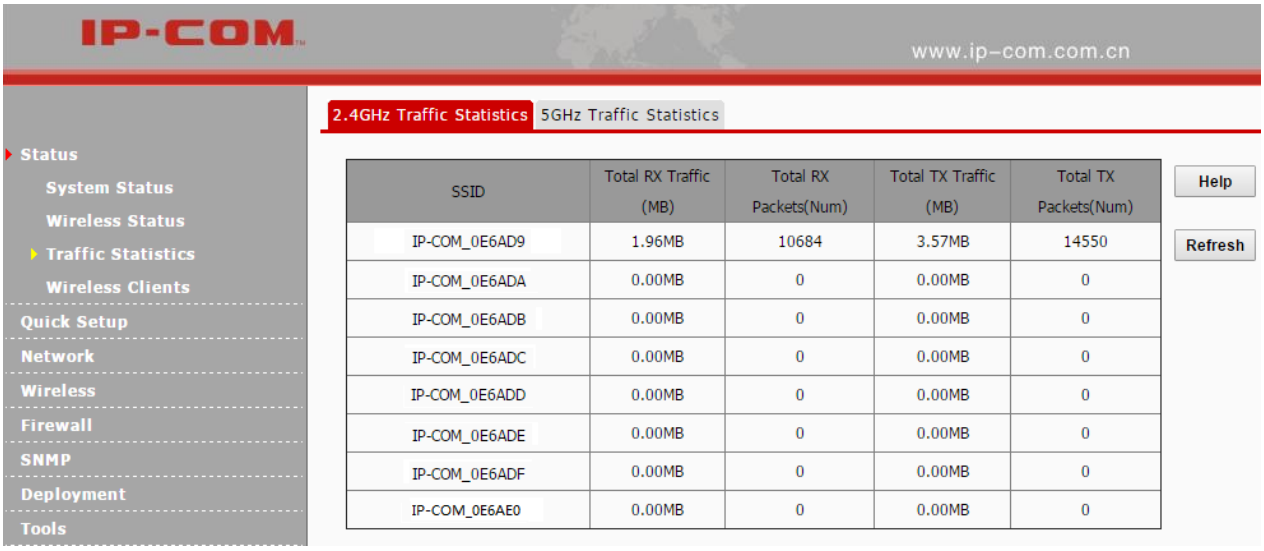
3.1.2 Wireless Status

This page displays radio status and SSID status at both 2.4GHz and 5GHz. Up to 8 SSIDs can be supported at 2.4GHz and 4 SSIDs can be supported at 5GHz. Click **Status > Wireless Status** to enter page below. To view 5GHz wireless status, click **5GHz Wireless Status**.



3.1.3 Traffic Statistics

This page displays total RX/TX traffic statistics and total RX/TX traffic packets of corresponding SSIDs. Click **Status** > **Traffic Statistics** to enter page below. To view 5GHz traffic statistics, click **5GHz Traffic Statistics**.

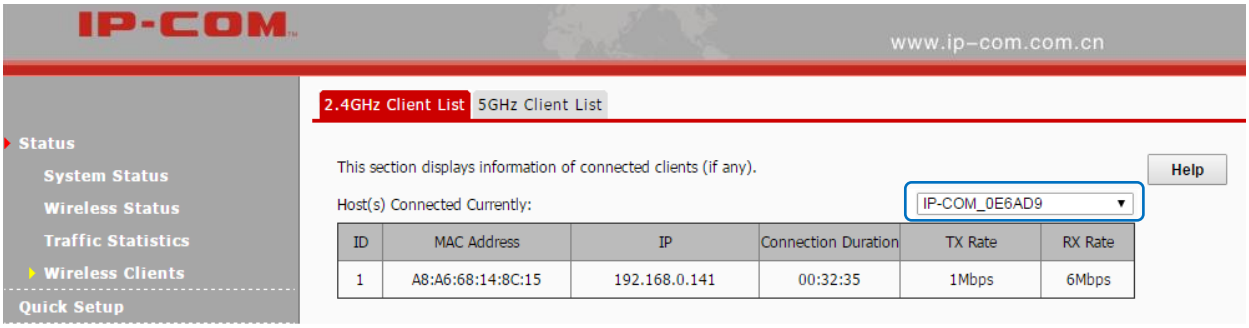


Click **Refresh** to view latest traffic statistics.

3.1.4 Wireless Clients

This page displays information, like MAC address, IP, connection duration and link speed of connected clients.

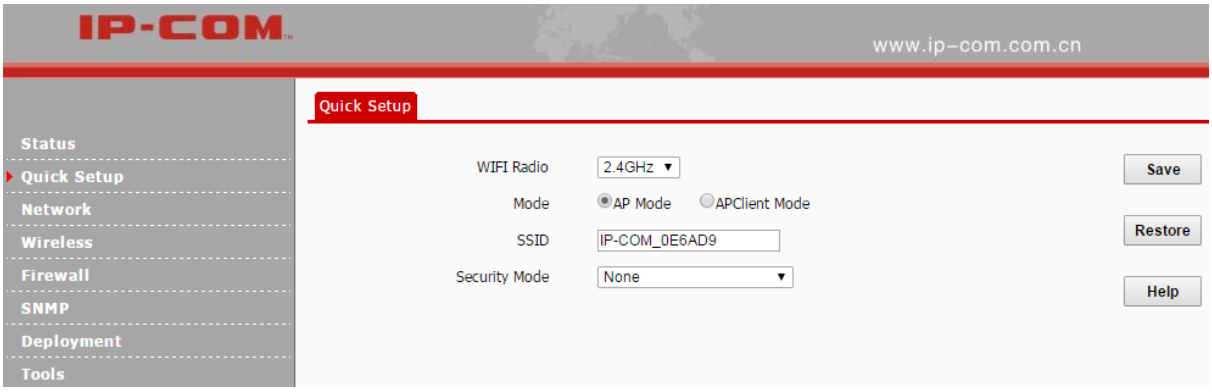
Click **Status > Wireless Clients** to enter page below. To view 5GHz client info, click **5GHz Client List**.



Click the drop-down menu at the top right corner and you can select to view the corresponding SSID's connected client info.

3.2 Quick Setup

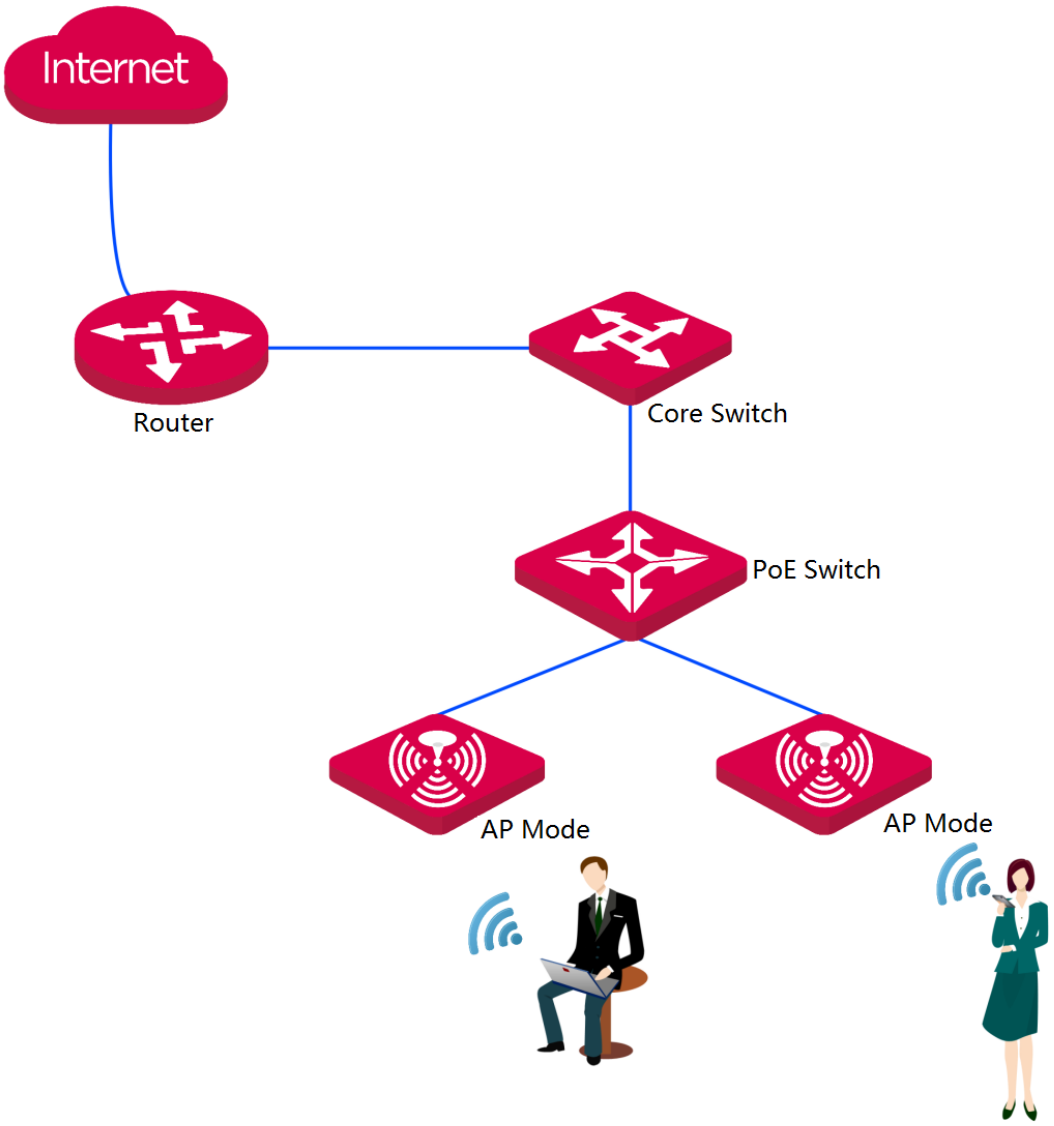
This section mainly walks you through operating modes of the AP. Click **Quick Setup** to enter page below and you can select the proper operating mode in terms of your network environment.



This AP supports 2 working modes: AP Mode and AP Client Mode. It's in AP Mode by default.

3.2.1 AP Mode

In this mode, the AP is connected to the Internet with an Ethernet cable, and converts the wired signal to wireless signal for wireless coverage. The network topology is shown as below:



Configuration Steps: (In this example, the wireless radio is 2.4GHz, security mode is Mixed WPA/WPA-PSK, and encryption type is AES. For other options, please refer to 3.4.1 SSID Setup.)

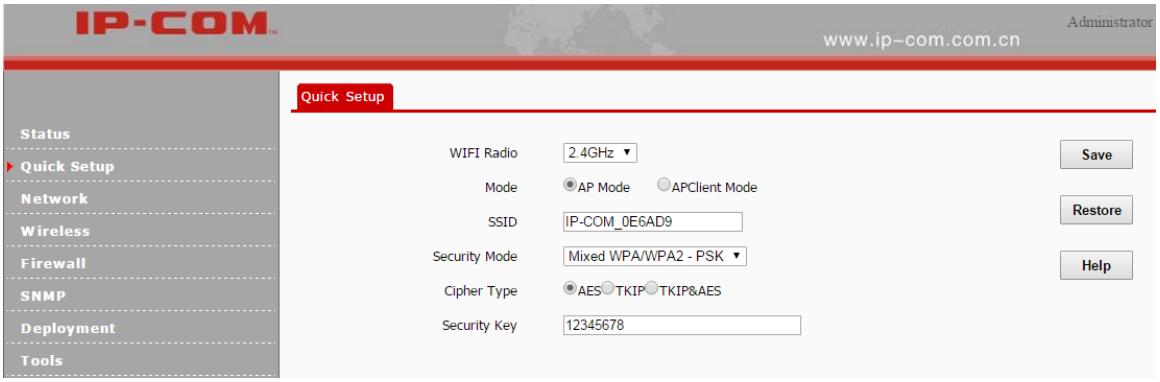
1. WiFi Radio: Select **2.4GHz**.

2. Mode: Select **AP Mode**.

3. SSID: Modify the SSID (optional). The SSID is the WiFi name you need to connect to for Internet access.

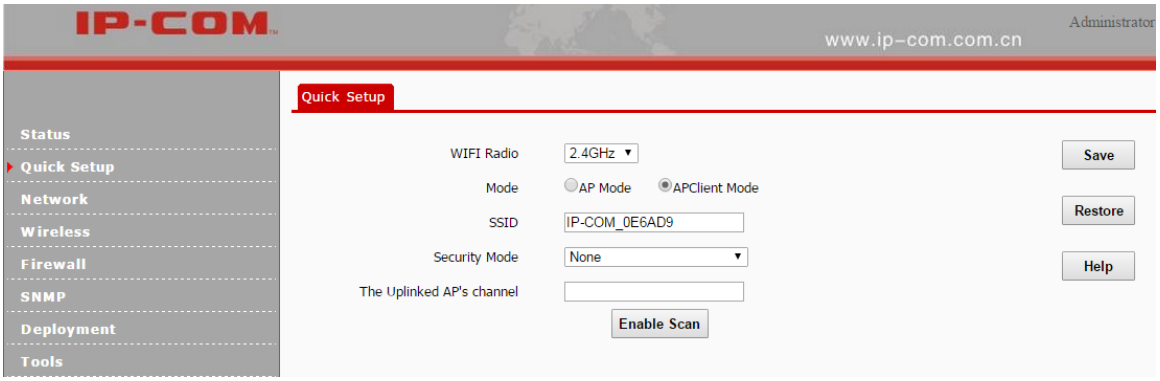
4. Security Mode: Select Mixed WPA/WPA2-PSK from the drop-down list, select AES, and customize a wireless password.

5. Click **Save** to apply your settings.



3.2.2 AP Client Mode

In this mode, the AP will be connected to the uplink router wirelessly, and expands the uplink signal for clients connected to the AP. Plus, configurations are only required on this AP.

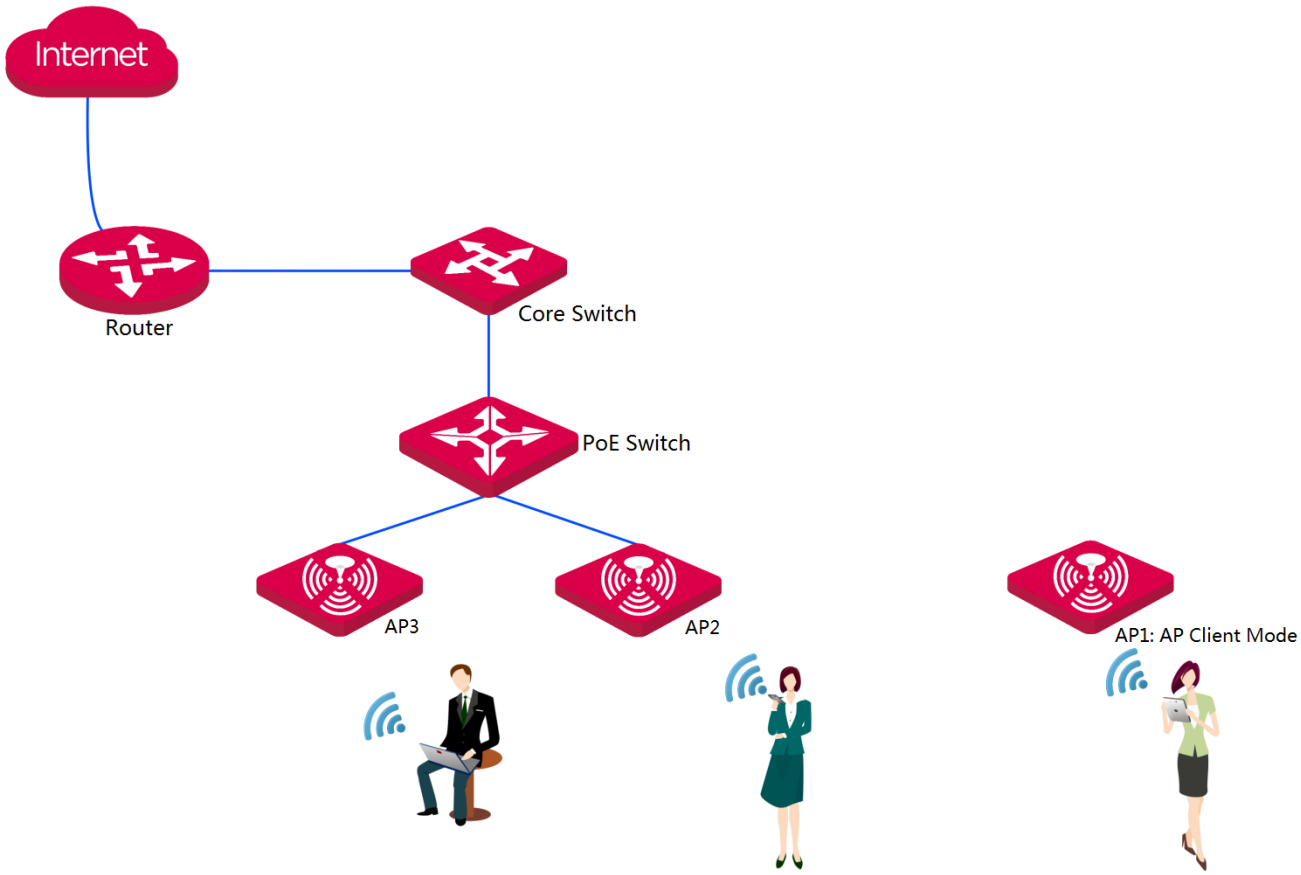


Application Scenario in AP Client Mode:

There's already an AP (Hereinafter referred as the remote AP) installed in a hotel. Due to limited WiFi coverage or other objects' intereference, some rooms of the hotel may be unable to enjoy WiFi smoothly.

Then you can install one more AP in the room where WiFi signal is not strong enough for WiFi extension with AP Client Mode. In this case, customers in distance can also enjoy the Internet.

You can take the following topology for reference.



Configuration Steps:

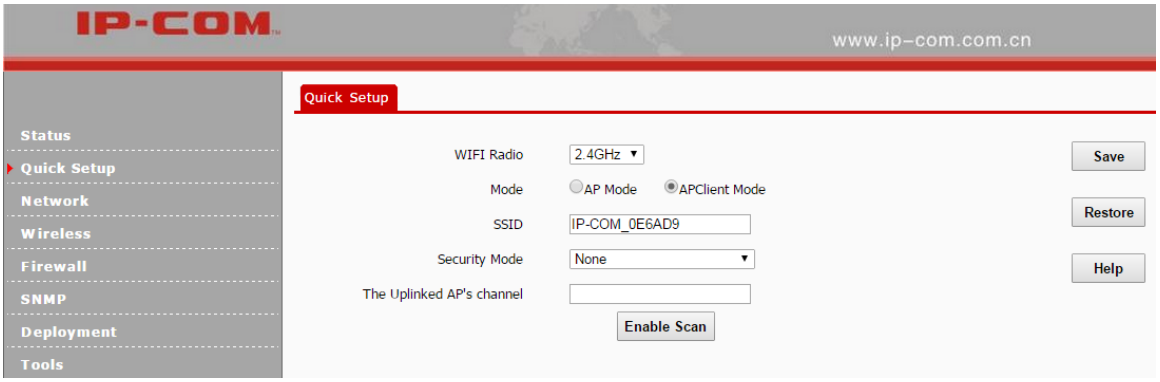
Assume that AP2 is the remote router as the topology displays.

1. Log in to the AP2's UI and note down the corresponding info. Assuming AP2's info is as below:

SSID	Security Mode	Key (WiFi password)	IP address
IP-COM_2	Mixed WPA/WPA2-PSK	86754321	192.168.0.254

2. Log in to the AP1's UI and set its IP address to one that is different from AP2 but on the same network segment, say, 192.168.0.253. For details, please refer to 3.3.1 LAN Setup.

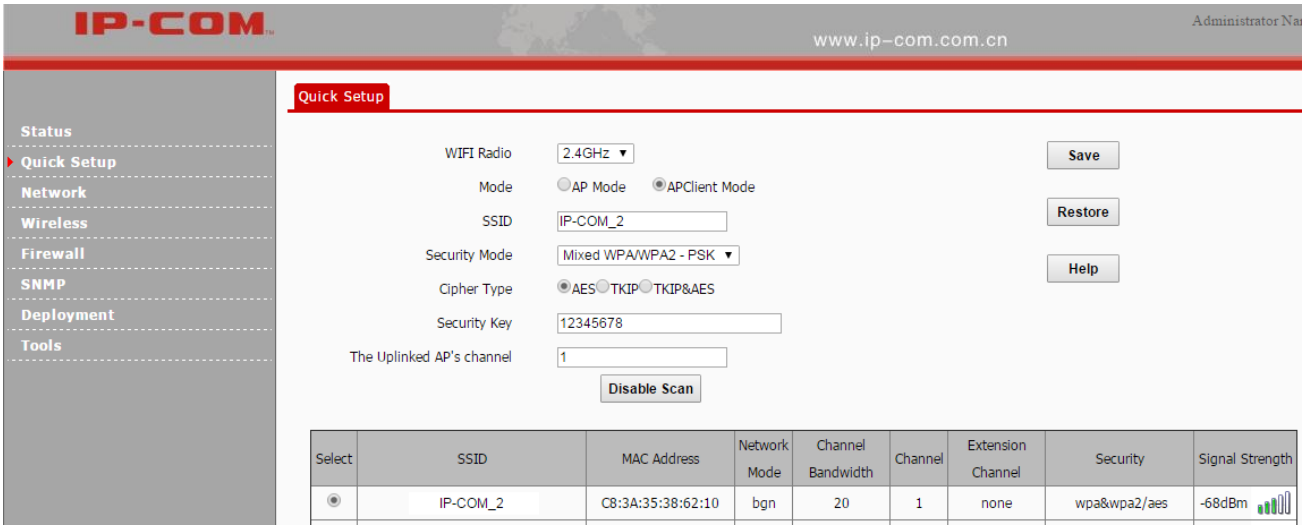
3. Re-log in to the AP1's UI with the new IP address, click **Quick Setup**, select **AP Client Mode** and click **Enable Scan**.



4. Select the AP2's SSID, IP-COM_2, in the list.

5. Security Key: Enter AP2's Key (WiFi password).

6. Click **Save** to apply your settings.



After AP1 has bridged to AP2 successfully, wireless clients, such as smart phones, can scan and connect to AP1's SSID, IP-COM_0E6AD9 in this case, for Internet access.

3.3 Network

This section consists of the following two parts:

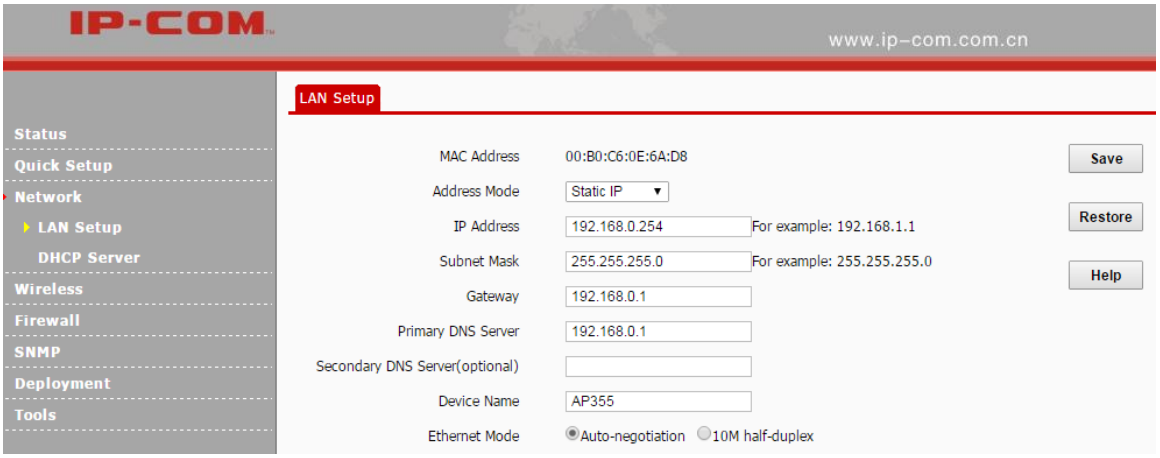
LAN Setup: Display the AP's MAC address of LAN port, support to configure the AP's IP info, device name and Ethernet Mode.

DHCP Server: Consist of DHCP Server and DHCP Client list.

3.3.1 LAN Setup

This section displays the AP's MAC address of LAN port and supports to configure the AP's IP info, device name and Ethernet Mode.

Click **Network** to configure LAN parameters.



This AP supports two address modes, **Static IP** and **Dynamic IP**, to obtain an IP address.

Tip

1. If the AP's IP address has changed, you need to change your PC's IP address to one that is different from the AP but on the same network segment, and re-log in to AP's UI with AP's new IP address.
2. By default, the AP's IP address is 192.168.0.254. It will be changed once managed by an AC successfully, and you can log in to AC's UI to check it.

Static IP

In this address mode, you need to configure the IP info manually. And it applies to small-scale network, where only several APs are deployed.

Configuration Steps:

1. Address Mode: Select **Static IP**.

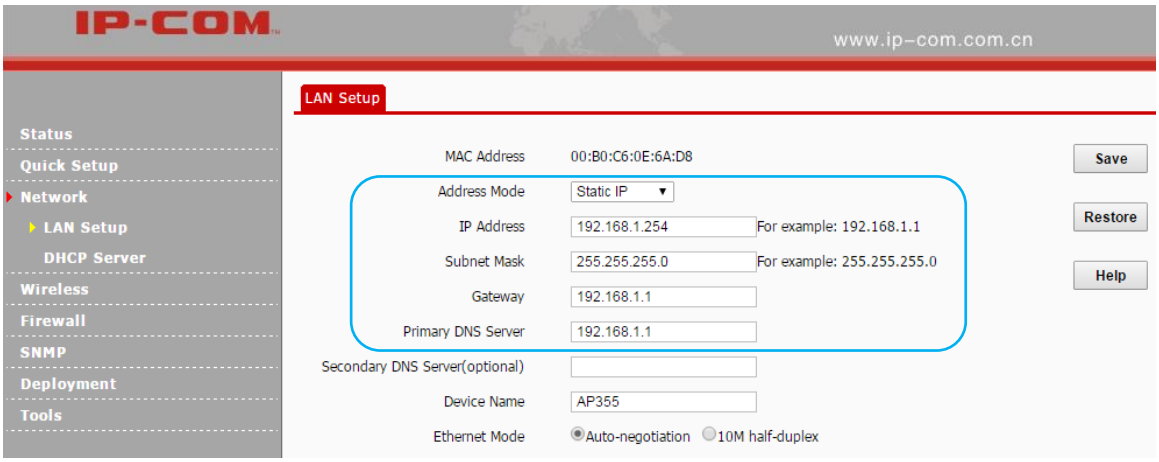
2. IP Address: Enter the AP's IP address, such as 192.168.1.254.

3. Subnet Mask: Enter the subnet mask of IP address. In general, it's 255.255.255.0.

4. Gateway: Enter the default gateway, such as 192.168.1.1.

5. Primary DNS Server: Enter the correct DNS IP address. The Secondary DNS Server is optional.

6. Click **Save** to apply your settings.



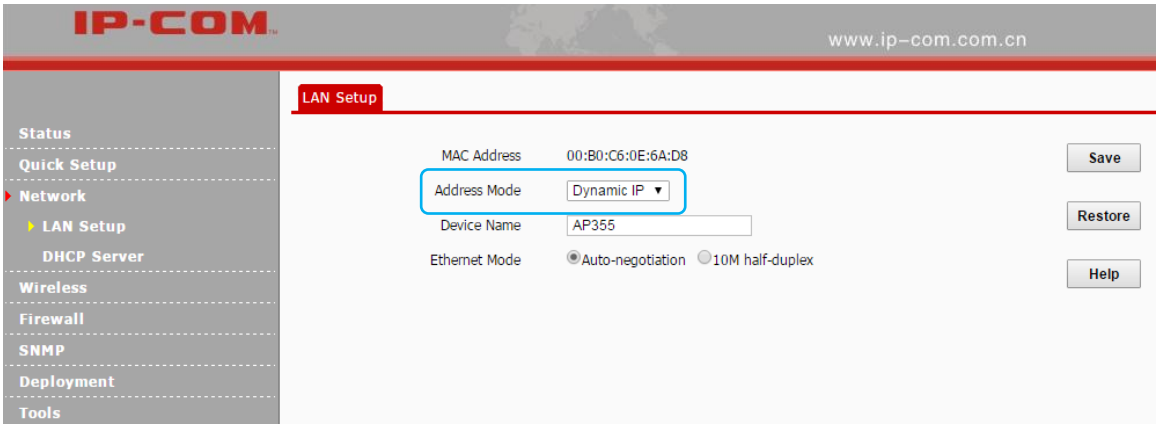
Dynamic IP

In this address mode, the AP will automatically get IP info, including IP address, subnet mask, gateway and primary/secondary DNS server, from the existing DHCP server. It applies to large-scale network, for avoiding IP collision and reducing workload of the administrator.

Configuration Steps:

1. Address Mode: Select **Dynamic IP**.

2. Click **Save** to apply your settings.



Parameters Description:

Item	Description
MAC address	AP's MAC address of LAN port. The primary SSID of the AP is IP-COM_XXXXXX, and XXXXXX is the last six characters of this MAC address.
Address Mode	Select the AP's address mode to obtain IP info. It's **Static IP** by default. • **Static IP**: Configure the AP's IP info manually, including IP address, subnet mask, gateway and DNS server. • **Dynamic IP**: The AP will automatically get IP info, including IP address, subnet mask, gateway and primary/secondary DNS server, from the existing DHCP server. **Tip** In **Dynamic IP** address mode, after the AP get IP info successfully, you need log in to the existing DHCP server' UI to check the AP's IP address in the DHCP Client List page. And re-log in to the AP's UI with the obtained IP address.
IP address	It's the AP's IP address for management. The computer in the same LAN with the AP can log in to the AP's UI with this IP address. In general, it is in the same network segment with the LAN IP address of gateway. **Tip** If the AP's IP address has changed, you need to change your PC's IP address to one that is different from the AP but on the same network segment, and re-log to AP's UI with AP's new IP address.
Subnet Mask	AP's subnet mask of IP address. It's 255.255.255.0 by default.
Gateway	In general, AP's gateway is the LAN IP address of the uplink router.
Primary DNS server	You need to enter the correct primary DNS IP address to ensure the AP's Internet service. If the uplink router is a DNS agent, this primary DNS server address can be the LAN IP address of the uplink router. If not, please enter the correct DNS server IP address.
Secondary DNS server (optional)	The secondary DNS server address is optional. If you have got two DNS server IP address, you can enter one of them here.
Device Name	By default, the AP's device name is the AP's model. It is recommended to change the device name.

Ethernet Mode	Transmission distance of its RJ45 port. The default value is Auto-negotiation, in which the Ethernet cable can be as long as 328 feet. The faster the auto-negotiation speed is, the shorter the transmission distance will be. When the AP can't communicate with its remote device, it is advisable to select 10M half-duplex mode.

3.3.2 DHCP Server

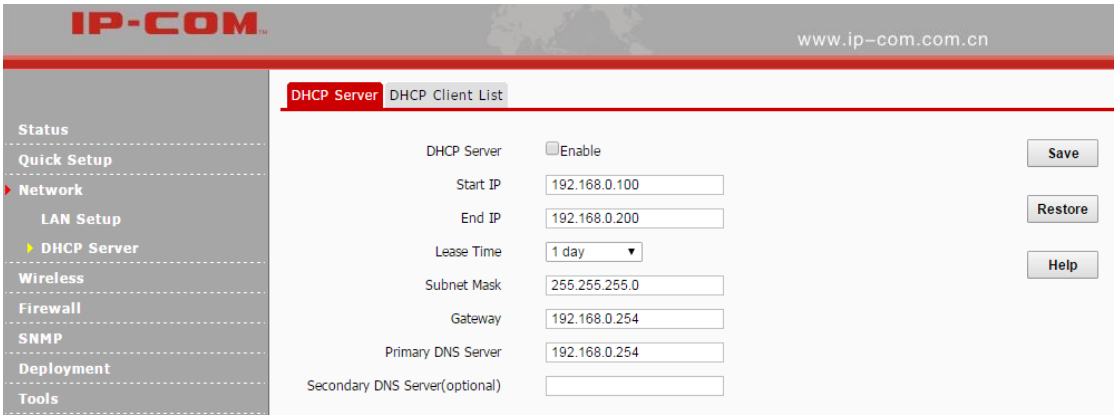
This AP has a built-in DHCP server, which is disabled by default. The following two parts are included:

DHCP Server: Configure relevant parameters of the DHCP server.

DHCP Client List: Display client info obtained from the DHCP server.

DHCP Server

If you enable the built-in DHCP server on the device, it will automatically configure the TCP/IP settings for all your LAN computers (including IP address, subnet mask, gateway and DNS etc.), eliminating the need of manual intervention. Just be sure to set all computers on your LAN to be DHCP clients by selecting **Obtain an IP Address Automatically** respectively on each PC. Click **Network > DHCP Server** to enter page below:



To enable the DHCP server:

1. DHCP Server: Check the **Enable** box to enable the DHCP server.

2. Start/End IP: Configure the start/end IP address of the address pool.

3. Lease Time: "1 day" is recommended.

4. Subnet Mask: "255.255.255.0" is recommended.

5. Gateway: Configure the default gateway IP that the DHCP server will assign to clients.

6. Primary/Secondary DNS Server: Configure the primary DNS server. If there's another DNS address, enter it in the Secondary DNS Server field.

7. Click **Save** to apply your settings.

Note

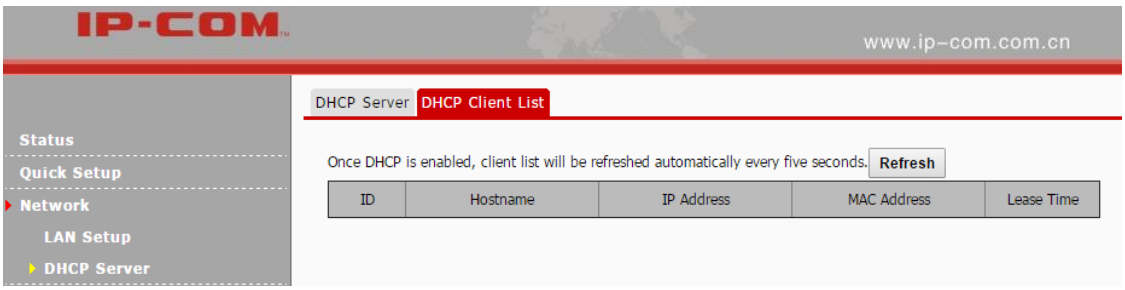
If there are other DHCP servers in the network, whether enable the DHCP server on the AP, depends on your actual needs. If you need to enable the DHCP server on the AP, to avoid IP conflicts, make sure that IP address pool of the AP is not overlapped with that of other DHCP servers.

Parameters Description:

Item	Description
DHCP Server	Check/Uncheck it to enable/disable the DHCP server. It is disabled by default.
Start IP	The start IP address that the DHCP server can assign to clients. By default, it is 192.168.0.100.
End IP	The end IP address that the DHCP server can assign to clients. By default, it is 192.168.0.200.
Lease Time	How long the IP address can be used by the client device. It is 1 day by default.
Subnet Mask	The subnet mask that the DHCP server will assign to clients. It is "255.255.255.0" by default.
Gateway	The default gateway IP that the DHCP server will assign to clients. It is "192.168.0.254" by default.
Primary DNS Server	Primary DNS server address. It is "192.168.0.254" by default. To ensure that the client can have an access to the Internet via the domain name, please enter the correct DNS server address.
Secondary DNS Server (optional)	Secondary DNS server address. It is an optional item.

DHCP Client List

Click **Network > DHCP Server > DHCP Client List** to view DHCP clients information.



Click **Refresh** to view the latest DHCP client info.

3.4 Wireless

This section allows you to configure wireless settings for your AP. The following parts are included:

SSID Setup: Configure basic SSID information for your AP, including SSID (WiFi name), clients, encryption information, etc.

Radio: Configure wireless radio information for your AP, including Enable/Disable WiFi, network mode, channel, etc.

Radio Optimizing: Optimize AP's wireless performance (For professional technical staffs).

Frequency Analysis: Give you an overview of background noise and channel utilization on each channel, and nearby wireless signals.

WMM Setup: Comfigure WMM settings.

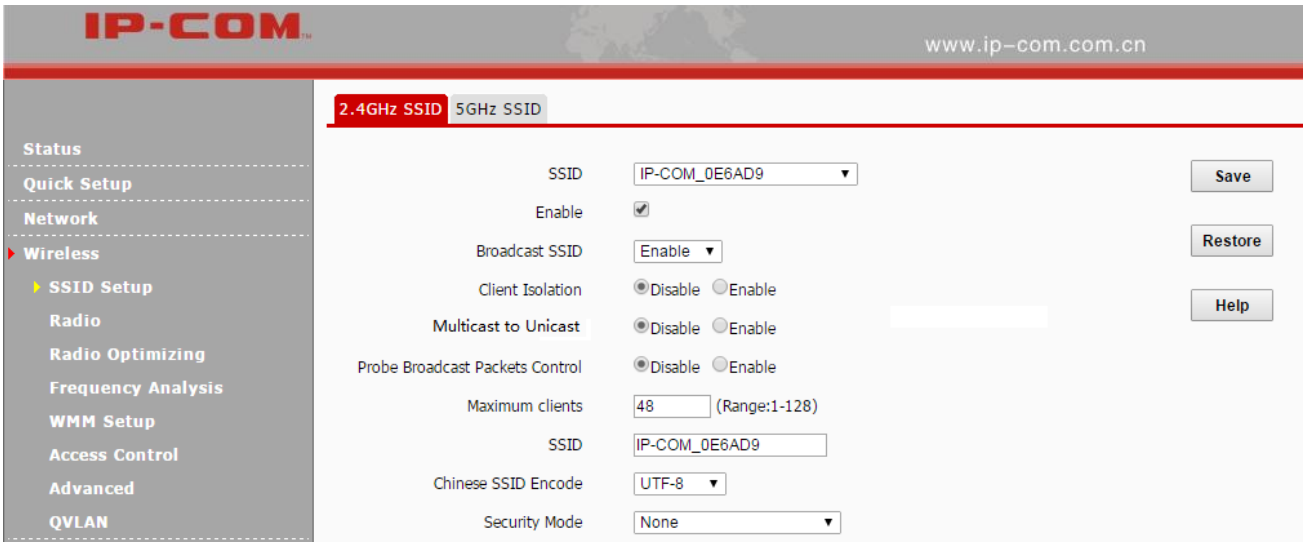
Access Control: Configure a list of devices to allow or disallow a connection to your WiFi via devices' MAC addresses.

Advanced: Configure to recognize terminal types and filter broadcast data.

QVLAN: Configure QVLAN settings to secure your WiFi.

3.4.1 SSID Setup

Click **Wireless** to configure basic SSID settings. To configure 5GHz SSID settings, click **5GHz SSID**.



Configuration steps for SSID settings:

If not necessary, leave other settings unchanged.

1. SSID: Click the drop-down menu to select the SSID you want to configure.

2. Enable: Check the **Enable** box to enable the selected SSID.

3. Configure the maximum number of wireless clients which can be allowed to connect to the SSID.

4. SSID: Modify the SSID (WiFi name).

5. Security Mode: Select a proper security mode for your SSID (For specific steps, see parameters described in the followings).

6. Click **Save** to apply your settings.

Parameters Description:

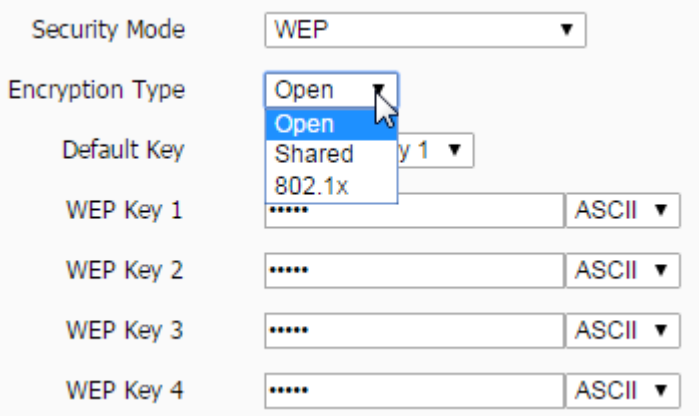
Item	Description
SSID	Select the SSID you want to configure. Up to 8 SSIDs at the 2.4GHz radio can be supported on this device. The default SSID is IP-COM_XXXXXX, which is the primary SSID of the AP at 2.4GHz. Up to 4 SSIDs at the 5GHz radio can be supported on this device. The default SSID is IP-COM-5G_YYYYYY, which is the primary SSID of the AP at 5GHz.
Enable	When you check it, Wi-Fi will be allowed for the selected SSID. By default, one SSID is enabled at both 2.4GHz and 5GHz, and other SSIDs are disabled.
Broadcast SSID	Configure the selected SSID's broadcast status. • Enable: When it is enabled, wireless clients are able to scan the SSID. • Disable: when it is disabled, wireless clients are unable to scan the SSID. At this time, if you want to connect to it wirelessly, you have to type in the SSID manually. **Tip** SSID can be hidden automatically on this AP. When the number of the maximum clients has been reached, the SSID will be hidden.
Client Isolation	Configure the client isolation status of the selected SSID. • Enable: When this feature is enabled, wireless clients connected to the SSID won't be able to communicate with each other, which can enhance wireless network security. • Disable: When this feature is disabled, Wireless clients connected to the SSID are able to communicate with each other.
Multicast to Unicast	Multicast to Unicast: Generally, multicast packets are usually transmitted at the lowest rate, like 1 Mbps. As unicast packets have advantages, like high auto-negotiation rate and reliable feedback mechanism, multicast-to-unicast can be a solution to packets drooping and large transmission delay.
Probe Broadcast Packets Control	Onec this feature is enabled, for probe request without SSID info, AP won't respond to it. In

	this way, it will efficiently reduce the consumption of the air interface.
Maximum Clients	Configure the maximum number of wireless clients which can connect to the SSID. When the number of connected wireless clients has reached this value, no more wireless clients can connect to the SSID.
SSID	Configure the SSID (WiFi name).
Chinese SSID Encode	Select Chinese SSID encodes to match wireless clients with different code formats in a better way. It is UTF-8 by default. If two or more SSIDs are enabled on this AP, it is advisable to set some SSIDs to UTF-8 and set others to GB2312 so that any client can recognize and connect to it.
Security Mode	Display wireless encryption information of the current SSID. Available security modes are: None, WEP, WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK, WPA, and WPA2. Next we will give you more details about them.

WEP

WEP (Wired Equivalent Privacy): WEP is a security mode for data which is delivered between two devices to protect wireless network from illegal users. Wireless speed can reach up to 54Mbps if WEP is used. For better network security, this kind of encryption is not suggested.

Three encryption types are supported for WEP: Open, Shared and 802.1x.



Tip

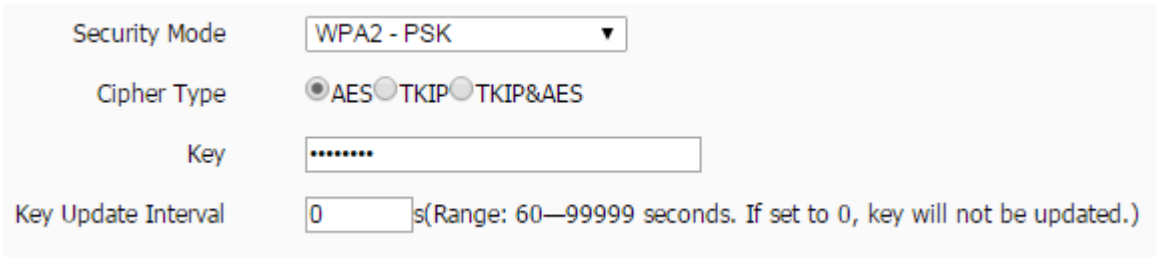
Most smart phones can only use WEP key 1 to connect to the WEP-encrypted (Open or Shared) WiFi. When the security mode is WEP, and the encryption type is Open or Shared, to verify that your smart phone can connect to the AP's WiFi, you'd better select WEP Key 1 as the default key.

Parameters description for WEP:

Item	Description
Encryption Type	Select the encryption type for WEP: Open, Shared or 802.1x. The only difference among them is the authentication type.
Open	Use "no authentication" + WEP Encryption. Wireless clients can associate with the device without authentication. Only data in transmission is encrypted with WEP encryption.
Shared	Use shared key authentication + WEP Encryption. A WEP key that is mutually agreed in advance is required from both sides while wireless clients try to associate with the device. Association is established only if the two sides provide the same WEP key.
802.1x	Use 802.1x authentication + WEP encryption. When this option is selected, only authenticated users can access the wireless network.
Default Key	Used for specifying the current WEP key (Open and Shared). If the default key is WEP Key 2, wireless clients need to use WEP Key 2 to connect to the AP.
ASCII	5~13 ASCII characters are supported.
Hex	10 or 26 HEX characters (0~9, a~f, A~F) are supported.
RADIUS Server	The IP address of the RADIUS server for authentication in the LAN. This option is only available for 802.1x.
RADIUS Port	Port for RADIUS authentication. This option is only available for 802.1x.
RADIUS Password	Password for accessing the RADIUS server. This option is only available for 802.1x.

WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. Only authorized network users can access the wireless network. WPA-PSK adopts enhanced encryption algorithm over WEP.

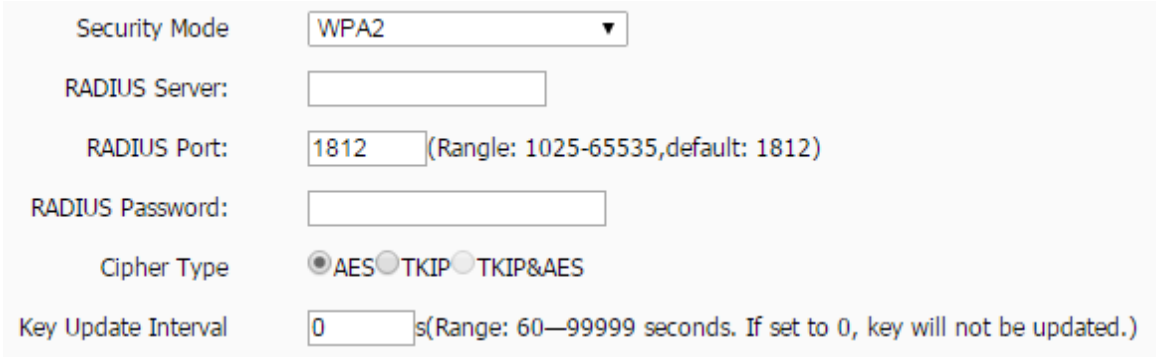


Parameters description for WPA-PSK, WPA2-PSK, Mixed WPA/WPA2-PSK:

Item	Description
Security Mode	Select the security mode: WPA-PSK, WPA2-PSK or Mixed WPA/WPA2-PSK.
WPA-PSK	Support AES and TKIP.
WPA2-PSK	Support AES, TKIP and TKIP&AES.
Mixed WPA/WPA2-PSK	This is the mixed mode compliant with both WPA-PSK and WPA2-PSK.
Cipher Type	Select the cipher type. WPA-PSK: AES and TKIP. WPA2-PSK and Mixed WPA/WPA2-PSK: AES, TKIP and TKIP&AES.
AES	Advanced Encryption Standard. If selected, wireless speed can reach up to 300Mbps.
TKIP	Temporal Key Integrity Protocol. If selected, wireless speed can reach up to 54Mbps.
TKIP&AES	If selected, both AES and TKIP enabled wireless clients can join your wireless network.
Key	Specify the security key you wish to configure (8~63 ASCII characters or 8~64 HEX characters).
Key Update Interval	Configure the key update interval for encrypting WPA data. Theoretically, the shorter the key update interval is, the more secure the WPA data will be. It is advisable to leave the default value unchanged.

WPA, WPA2

The WPA protocol implements the majority of the IEEE 802.11i standard. It enhances data encryption through the Temporal Key Integrity Protocol (TKIP) which is a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. WPA also includes a message integrity check feature to prevent data packets from being hampered with. Only authorized network users can access the wireless network. The later WPA2 protocol features compliance with the full IEEE 802.11i standard and uses Advanced Encryption Standard (AES) in addition to TKIP encryption protocol to guarantee better security than that provided by WEP or WPA.



Parameters description for WPA, WPA2:

Item	Description
Security Mode	Select the security mode, WPA or WPA2.
WPA	Support AES and TKIP.
WPA2	Support AES, TKIP and TKIP&AES.
RADIUS Server	The IP address of the RADIUS server for authentication in the LAN.
RADIUS Port	Port for RADIUS authentication.
RADIUS Password	Password for accessing the RADIUS server.
Cipher Type	Support AES, TKIP and TKIP&AES.
AES	Advanced Encryption Standard. If selected, wireless speed can reach up to 300Mbps.
TKIP	Temporal Key Integrity Protocol. If selected, wireless speed can reach up to 54Mbps.
TKIP&AES	If selected, both AES and TKIP enabled wireless clients can join your wireless network.
Key Update Interval	Configure the key update interval for encrypting WPA data. Theoretically, the shorter the key update interval is, the more secure the WPA data will be.

Configuration steps for Open/Shared:

In this example, the radio is 2.4GHz, the encryption type is Open, the default key is Security Key 1 and the WEP key 1 is 54321 and ASCII)

1. SSID: Select the SSID (WiFi name) you want to encrypt, say, IP-COM_0E6AD9.

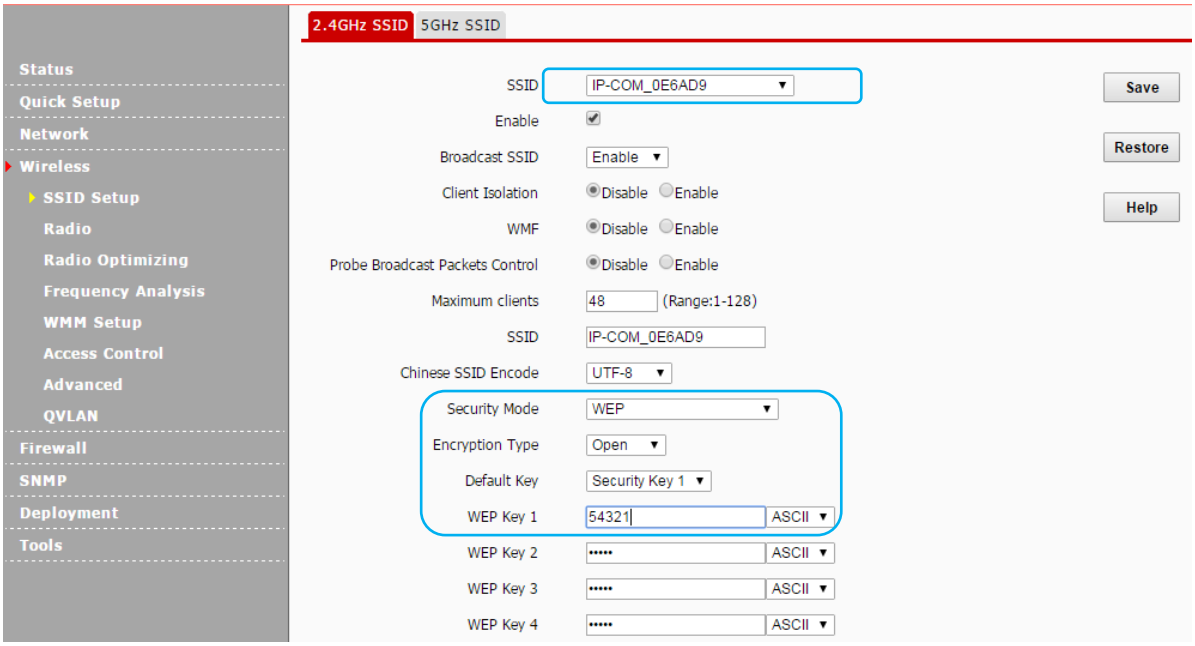
2. Security Mode: Select **WEP**.

3. Encryption Type: Select **Open**.

4. Default Key: Select **Security Key 1**.

5. WEP Key 1: Enter “54321”.

6. Click **Save** to apply your settings.



Configuration steps for 802.1x:

In this example, the radio is 2.4GHz, the RADIUS server is 192.168.0.88, the RADIUS port is 1812 and its password is 12345678.

1. SSID: Select the SSID you want to encrypt, say, IP-COM_0E6AD9.

2. Security Mode: Select **WEP**.

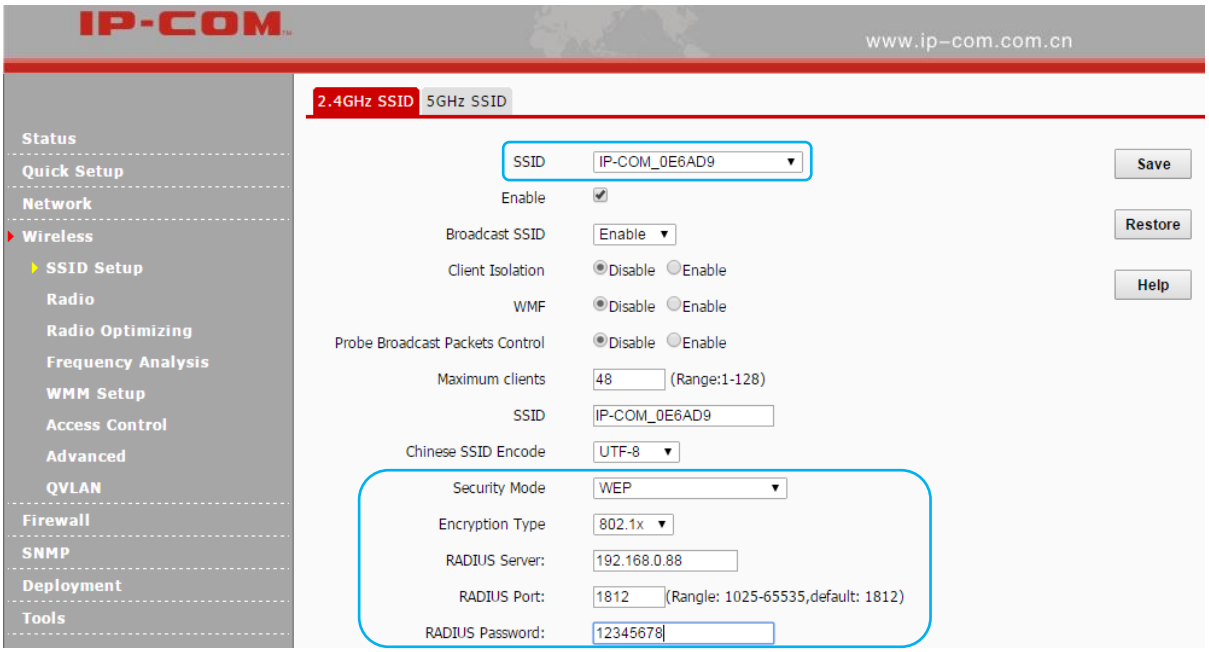
3. Encryption Type: Select **802.1x**.

4. RADIUS Server: Enter the IP address of the radius server, say, 192.168.0.88.

5. RADIUS port: Enter 1812 (The default value is suggested).

6. RADIUS password: Enter 12345678.

7. Click **Save** to apply your settings.



Configuration steps for WPA-PSK, WPA2-PSK, mixed WPA/WPA2-PSK:

In this example, the radio is 2.4GHz, the security mode is mixed WPA/WPA2-PSK, the cipher type is AES and its key is 12345678.

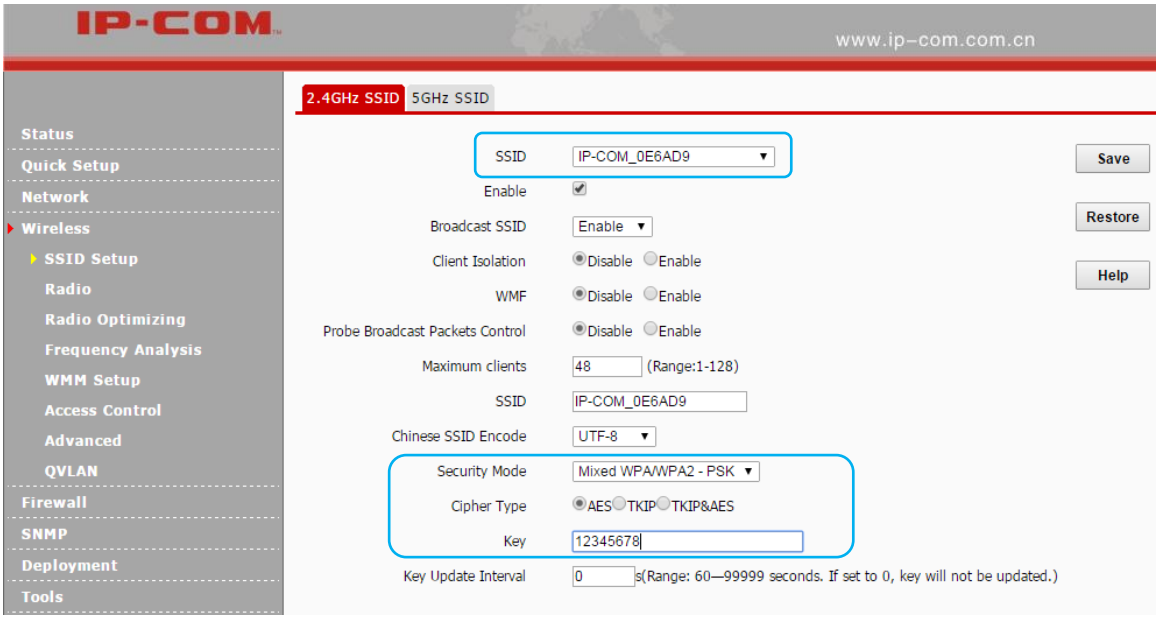
1. SSID: Select the SSID you want to encrypt, say "IP-COM_0E6AD9".

2. Security Mode: Select **Mixed WPA/WPA2-PSK**.

3. Encryption Type: Select **AES**.

4. Key: Enter 12345648.

5. Click **Save** to apply your settings.



Configuration Steps for WPA, WPA2:

In this example, the radio is 2.4GHz, the RADIUS server is 192.168.0.88, the RADIUS port is 1812, the RADIUS password is 12345678, and the cipher type is AES.

1. SSID: Select the SSID you want to encrypt, say, IP-COM_0E6AD9.

2. Security Mode: Select **WPA**.

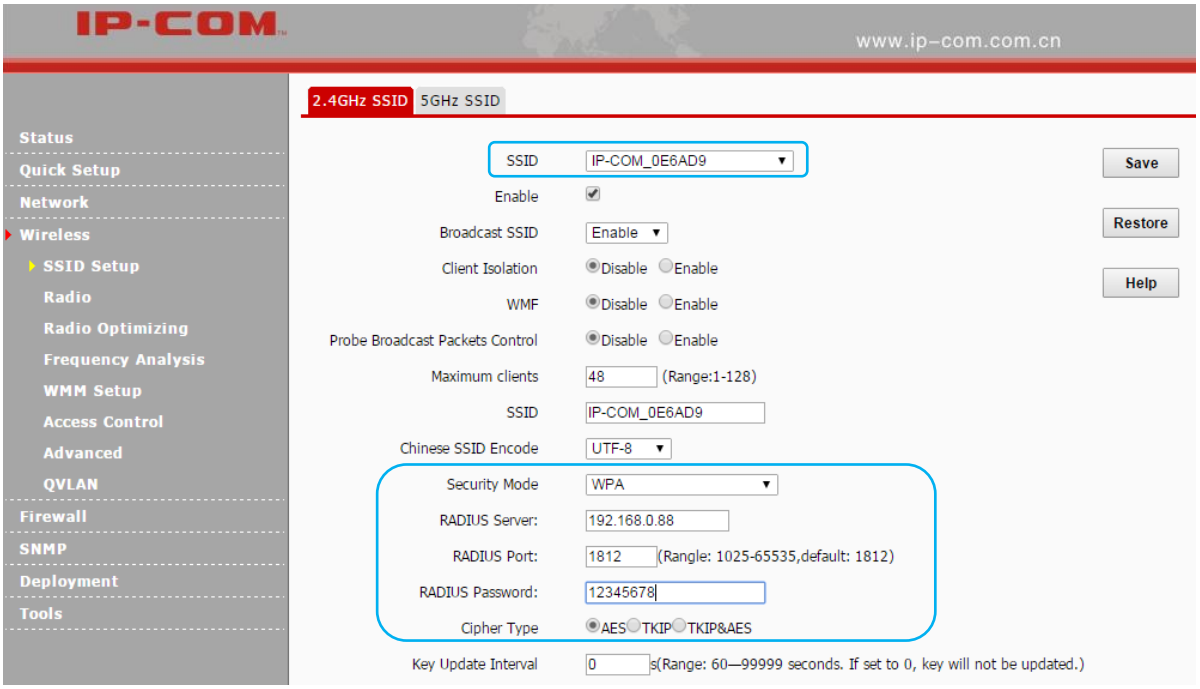
3. RADIUS Server: Enter the IP address of the radius server, say, 192.168.0.88.

4. RADIUS Port: Enter 1812 (The default value is suggested).

5. RADIUS password: Enter 12345678.

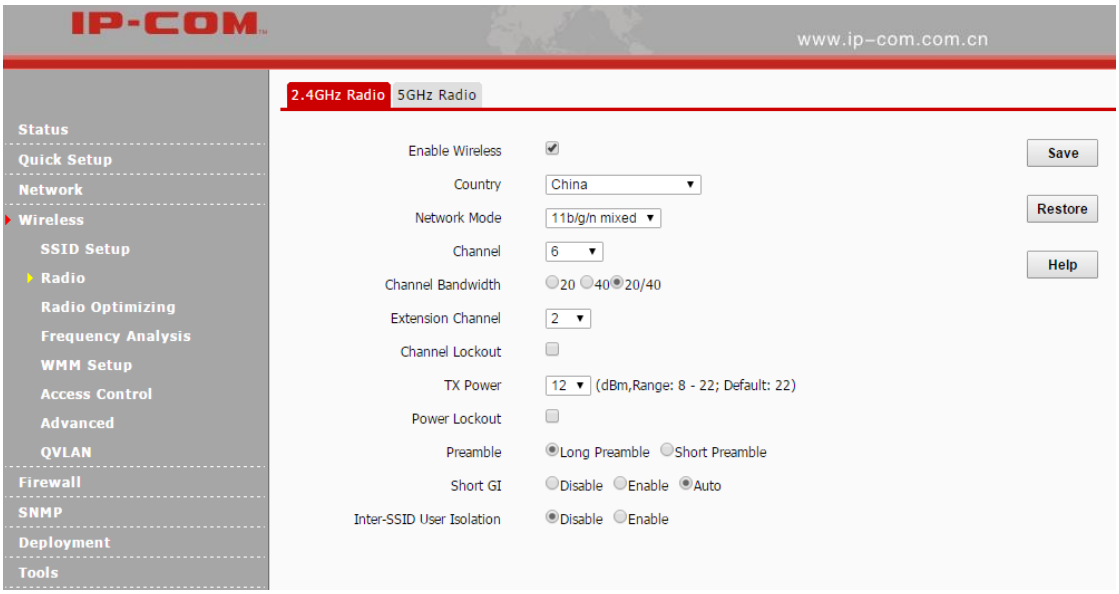
6. Cipher Type: Select **AES**.

7. Click **Save** to apply your settings.



3.4.2 Radio

Click **Wireless > Radio** to configure radio settings. To configure 5GHz radio settings, click **5GHz Radio**.



Parameters Description:

Item	Description
Enable Wireless	Check/Uncheck it to enable/disable WiFi feature.
Country	Select the country where your device works to match channels in different regions.

Network Mode	Select a proper network mode for your device. **11b, 11g, 11b/g and 11b/g/n are available for 2.4GHz.** • 11b: Select it if you have only 11b wireless devices in your wireless network. Up to 11Mbps wireless rate is supported in this mode. • 11g: Select it if you have only 11g wireless devices in your wireless network. Up to 54Mbps wireless rate is supported in this mode. • 11b/g: Select it if you have 11b and 11g wireless devices in your wireless network. Up to 54Mbps wireless rate is supported in this mode. • 11b/g/n: Select it if you have 11b, 11g and 11n wireless devices in your wireless network. Up to 300Mbps wireless rate is supported in this mode. **11a, 11ac and 11a/n are available for 5GHz.** • 11a: Select it if you have only 11a wireless devices in your wireless network. Up to 54Mbps wireless rate is supported in this mode. • 11ac: Select it if you only have 11ac wireless devices in your wireless network. Up to 900Mbps wireless rate is supported in this mode. • 11a/n: Select it if you have 11a and 11n wireless devices in your wireless network. Up to 300Mbps wireless rate is supported in this mode.
Channel	Select a proper channel for your wireless network.
Channel Bandwidth	Select a proper channel bandwidth to enhance wireless performance. Wireless speed in the channel bandwidth of 20/40 is 2 times in 20.
Extension Channel	This item is available when the bandwidth is 40.
Channel Lockout	Once this option is enabled, you can’t modify the country, channel, channel bandwidth and extension channel manually.
TX Power	Configure wireless transmission power. The higher the TX power is, the wider the AP’s WiFi coverage will be. However, reducing the TX power to some extent will be helpful for your wireless performance and network security.
Power Lockout	Once this option is enabled, you can’t modify power manually.
Preamble	Preamble is used to synchronize a data transmission by indicating the end of header information and the start of data. There are two types of preambles: long preamble and short preamble. • Long Preamble: It can be compatible with some old wireless adapters.

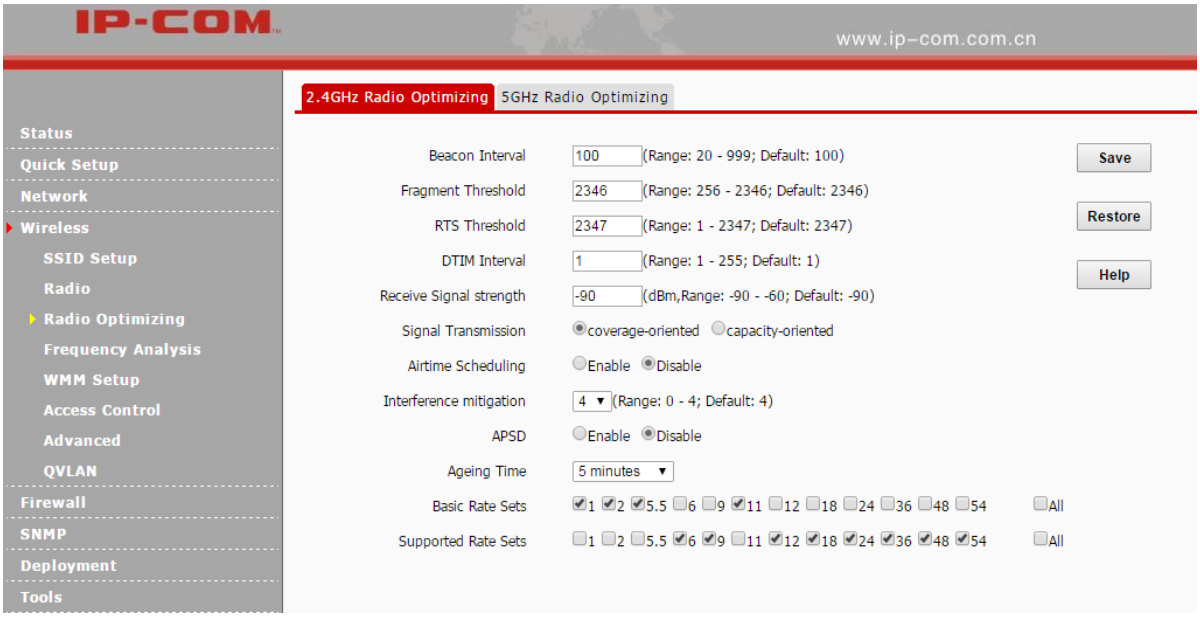
	• Short Preamble: The longer the preamble is, the shorter valid data will be. The short preamble can help to enhance wireless transmission efficiency.
Short GI	The purpose of the guard interval is to introduce immunity to propagation delays, echoes and reflections, to which digital data is normally very sensitive. Enabling the short GI can yield a 10% improvement in data throughput. When Auto is selected, whether Short GI is enabled or disabled, it depends on its actual networking environment.
Inter-SSID User Isolation	Configure the AP's different SSIDs' user isolation status. • Disable: Once disabled, clients connect to different SSIDs can't communicate with each other. This will enhance your network security. • Enable: Once enabled, clients connect to different SSIDs can communicate with each other.

3.4.3 Radio Optimizing

Click **Wireless > Radio Optimizing** to optimize radio settings. To optimize 5GHz radio settings, click **5GHz Radio Optimizing**.

Note

If you are new to networking and have never configured these settings before, we recommend you to leave the default settings unchanged.



Parameters Description:

Item	Description

Beacon Interval	This is a time interval between any two consecutive Beacon packets sent by an Access Point to synchronize a wireless network. Specify a valid value between 20 and 999. The default setting is 100. Generally, the smaller the value is, the faster the client will connect to the AP; the larger the value is, the faster the wireless data will be transmitted. It is advisable to leave the default value unchanged.
Fragment Threshold	Specify a valid Fragment Threshold value between 256 and 2346. The default is 2346. Any wireless packet exceeding the preset value will be divided into several fragments before transmission. When the error rate is relatively high, you can lower the fragment threshold. In this way, if transmission failure occurs, only packets that are not sent successfully needs re-sending, which will improve the transmission throughput. With no interference, you can improve the fragment threshold to reduce times to acknowledge frames, also improving the transmission throughput.
RTS Threshold	The default is 2347. If a packet exceeds the preset value, RTS/CTS scheme will be used to reduce collisions. Set it to a smaller value provided that there are distant clients and interference. If the RTS threshold value is relatively small, the wireless access point uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism, and the data frame is transmitted immediately after the silence period. The faster the frame is sent, the faster the wireless network will recover from collisions. As the collision detection mechanism will occupy some bandwidths, when the packet size is less than the RTS threshold, it is not advisable to enable this mechanism.
DTIM Interval	A DTIM (Delivery Traffic Indication Message) Interval is a countdown informing clients of the next window for listening to broadcast and multicast messages. When such packets arrive in the router's buffer, the router will send DTIM (delivery traffic indication message) and DTIM interval to alert clients of the receiving packets. Specify a valid value between 1 and 255. The default is 1. Fox example, when the DTIM is 1, it means that the AP will send all cached packets every other Beacon interval.
Receive Signal strength	Configure signal strength for connected clients. When the wireless client’s signal strength is lower than the setting value, the wireless client will not be allowed to connect to the AP so that the wireless client can connect to a stronger WiFi.
5GHZ SSID Priority	This option is only available at 5GHz. When there are 2 SSIDs with the same SSID and password, one at 2.4GHz, and the other at 5GHz, and the client support 2.4GHz and 5GHz, the client will take its priority to connect to the SSID at 5GHz. In this case, only WPA/WPA2-PSK and Mixed WPA/WPA2-PSK are supported.
5GHZ Threshold	This option is available when 5GHz SSID Priority is enabled. The AP will check the receive signal strength at 5GHz. If the receive signal strength is

	lower than the threshold value at 5GHz, the client will not be allowed to connect to the AP.
Signal Transmission	This item is only available at 2.4GHz. • Coverage-oriented: When coverage-oriented is selected, the AP's WiFi coverage will be wider. • Capacity-oriented: When you deploy many APs in your network, capacity-oriented option is recommended.
Airtime Scheduling	Airtime Scheduling gives equal amounts of air time (instead of equal number of frames) to each client regardless of its theoretical data rate. This will ensure higher download speed to latest devices when slower devices are connected to the same AP.
Interference mitigation	Interference mitigation: interference mitigation mode, range: 0-4. The default is 4. This is only available in 2.4GHz. • 0: All interference mitigation is disabled. • 1: Non-wireless LAN Interference mitigation is enabled. • 2: Wireless LAN Interference mitigation is enabled. • 3: Auto Wireless LAN Interference mitigation is enabled and active. • 4: Auto Wireless LAN Interference mitigation is enabled and noise reduction is enabled.
APSD	Automatic power save delivery. It is advisable to keep the default value unchanged.
Ageing Time	When the client connects to the AP successfully, and if there's no data transmission between the client and the AP within the set ageing time, the client will be disconnected. If there's data transmission within the set ageing time, the ageing time stops.
Basic Rate Sets, Supported Rate Sets	• Basic Rate Sets: Check the transmission rate sets you want the AP to advertise. Basic rate sets indicate rates that the AP will advertise to the network for the purposes of setting up communication with other APs and client stations on the network. • Supported Rate Sets: Check the transmission rate sets you want the AP to support. The AP will automatically choose the most efficient rate based on factors like error rates and distance of client stations from the AP.

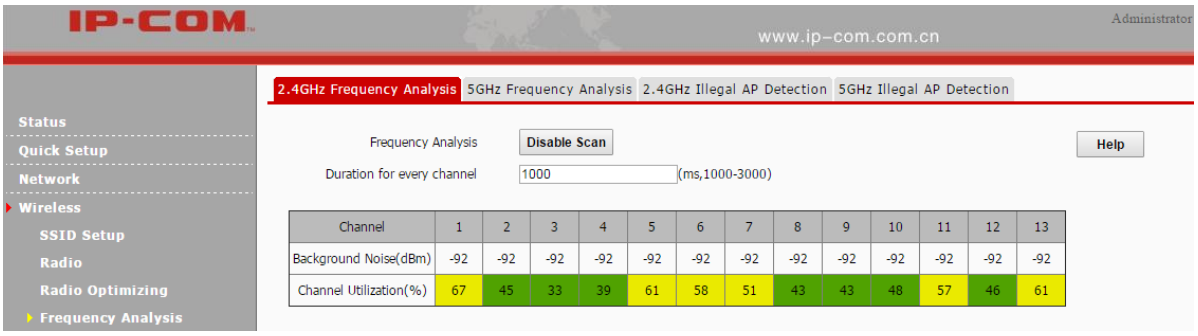
3.4.4 Frequency Analysis

This section allows you to view background noise and channel utilization on each channel, and nearby wireless signals.

2.4GHz & 5GHz Frequency Analysis

Click **Wireless > Frequency Analysis** to enter page below, and then click **Enable Scan** to view 2.4GHz frequency analysis. To view 5GHz frequency analysis, click **5GHz Frequency Analysis**.

Click **Enable Scan**, wait for a while, and then you can view background noise and channel utilization on each channel. You can select a channel whose utilization is relatively low as the AP's working channel.



If the channel utilization is 0~50%, it will display in green, indicating the channel is in good condition. If the channel utilization is 50%~80%, it will display in yellow, indicating the congested channel. If the channel utilization is 80%~100%, it will display in red, indicating no more available channel.

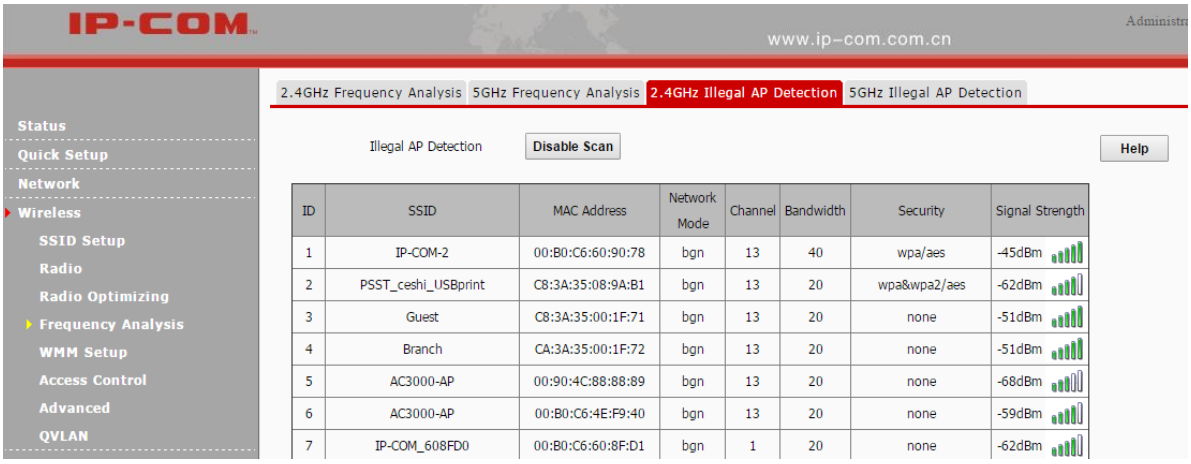
Parameters Description:

Item	Description
Duration for every channel	Time for every channel when scaning.
Background Noise	It refers to all kinds of electromagnetic waves in wireless communication. If there's much noise, data transmission may be affected.

2.4GHz & 5GHz Illegal AP Detection

This is mainly used for scaning signal of other devices nearby, displaying SSID, MAC, channel, signal strength, etc. To view 2.4GHz illegal AP detection, click **Wireless > Frequency Analysis > 2.4GHz Illegal AP Detection**, and then click **Enable Scan** on the pop-out page; To view 5GHz illegal AP detection, click **Wireless > Frequency Analysis > 5GHz Illegal AP Detection**, and then click **Enable Scan** on the pop-out page.

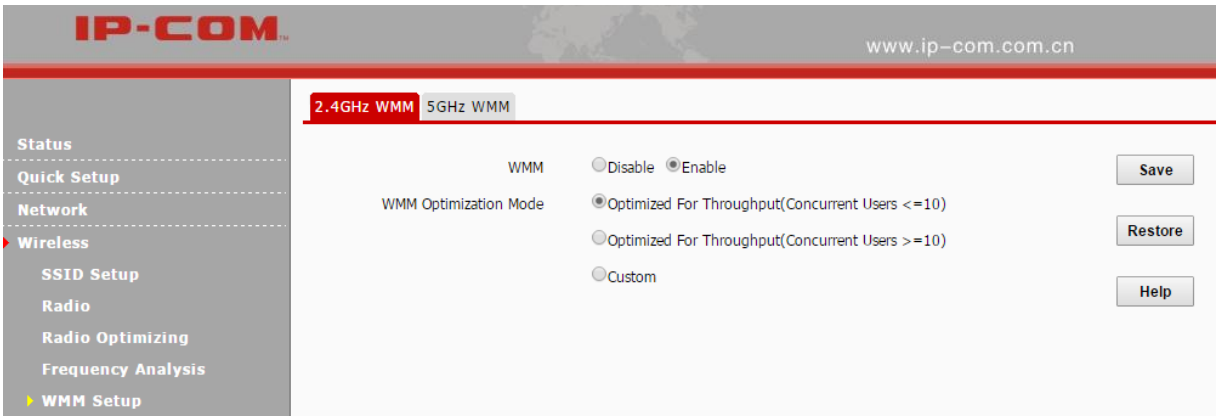
According to the list you've scanned, you can select a channel which is least used by other devices, so that wireless transmission efficiency can be improved.



3.4.5 WMM Setup

WMM (Wi-Fi Multimedia) is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks.

Click **Wireless > WMM Setup** to enter page below:



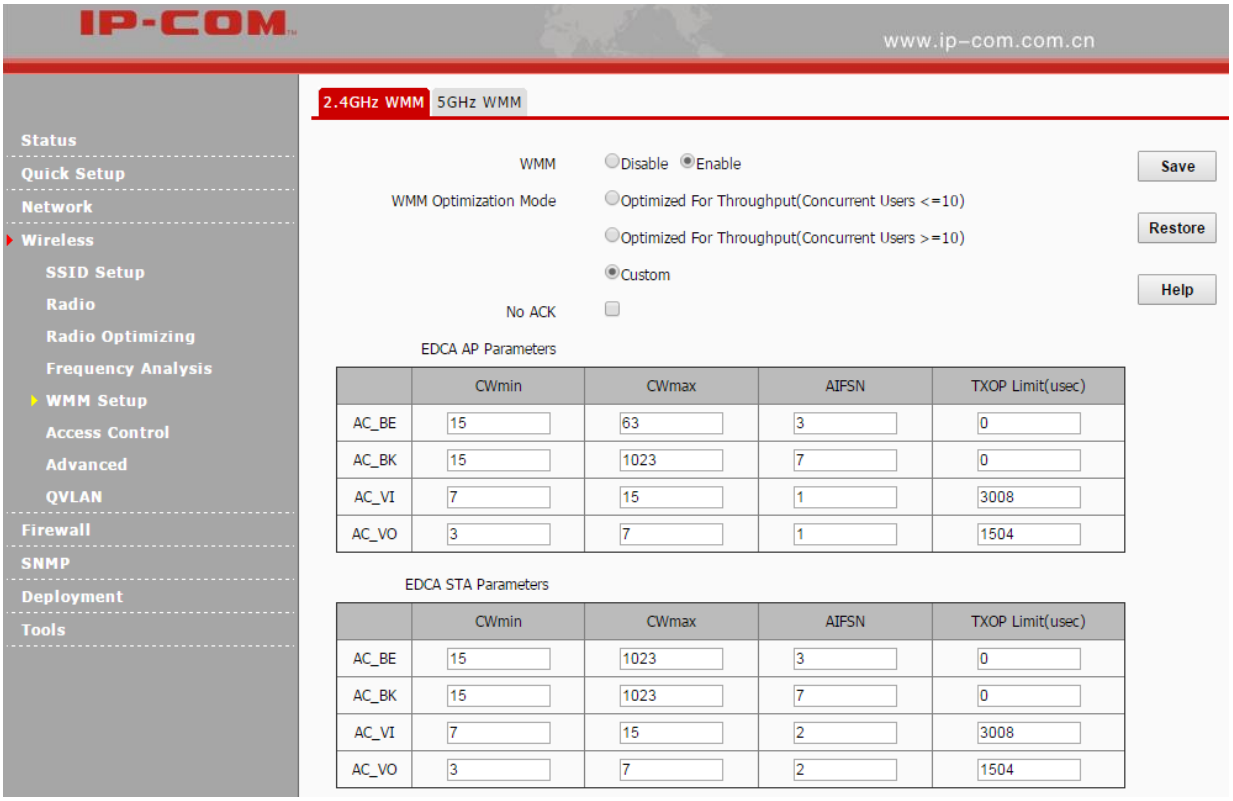
By default, WMM is enabled and three application modes are available:

- Optimized for Throughput (Concurrent Users <=10): If the number of Concurrent Users is less than 10, “Optimized for Throughput” template is recommended.
- Optimized for Capacity (Concurrent Users >=10): If the number of Concurrent Users is more than 10, “Optimized for Capacity” template is recommended.
- Custom: You can customize the WMM EDCA parameters. For more details, see description below.

Description for WMM EDCA:

If Custom is selected, the following page will pop-out.

WMM prioritizes traffic according to four Access Categories (AC) – voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK). If you are not familiar with these parameters, leave the default setting unchanged.



Parameters Description:

Item	Description
No ACK	No ACK is a kind of policy to be used only while the network communication is in good condition with little interference. To some extent, No ACK can improve transmission efficiency. But, if the communication quality is not good, packets dropping may increase.

EDCA	EDCA (Enhanced Distributed Channel Access) is a channel contention mechanism defined by WMM, so that packets which have high priority can be transmitted in advance and get more bandwidth.
EDCA AP Parameters	EDCA parameters of the AP.
EDCA STA Parameters	EDCA P parameters of the station.
EDCA Parametrs	• CWmin: Exponent form of CWmin • CWmax: Exponent form of CWmax CW: contention window. CWmin (Exponent form of Cwmin) and CWmax (Exponent form of Cwmax) codetermine average backoff time. The greater these two values are, the longer the average backoff time will be. • AIFSN (Arbitration Inter Frame Spacing Number): According to WMM, different ACs can have different idle waiting time. The greater the AIFSN value is, the longer the idle waiting time will be. • TXOP Limit (Transmission Opportunity Limit): The maximum use time for the channel for the user while contending successfully. The greater the value is, the longer the channel can be used by the user. If it is set to “0”, only one packet can be sent every time the channel is used.
AC_BE, AC_BK, AC_VI, AC_VO	4 priority queues are ranked from high to low by WMM: AC-VO, AC-VI, AC-BE and AC-BK to ensure that packets with higher priority have more abilities to occupy channels.

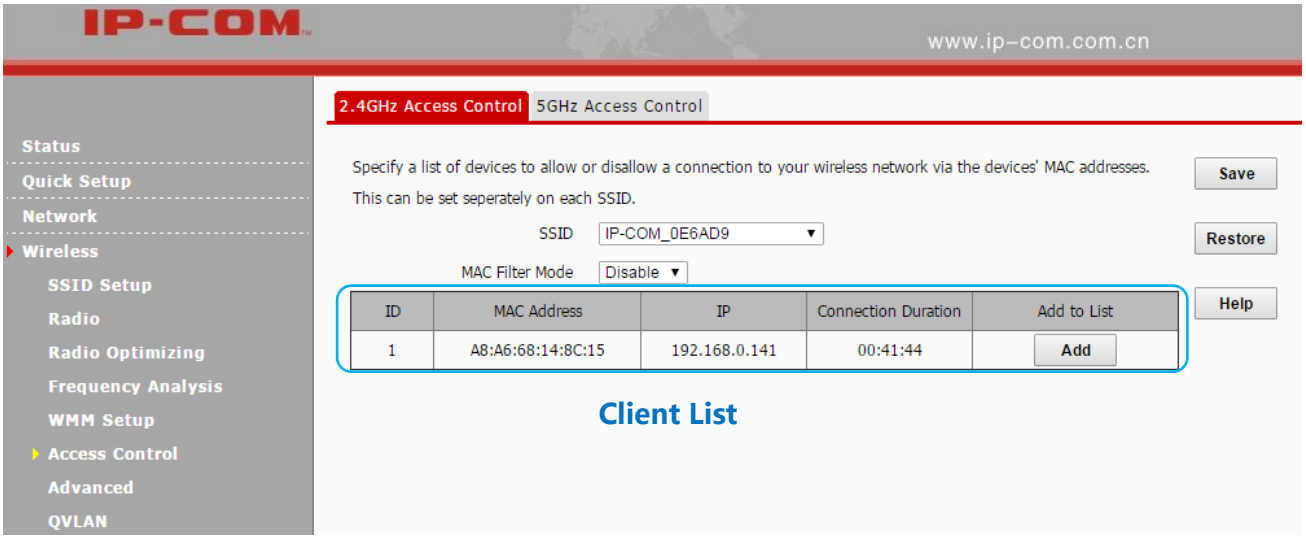
3.4.6 Access Control

Click **Wireless > Access Control** to enter page below. This page allows you to specify a list of devices to allow or disallow a connection to your wireless network via the devices’ MAC addresses. To deactivate this feature, select "Disable"; to activate it, select "Allow" or "Deny".

Parameters Description:

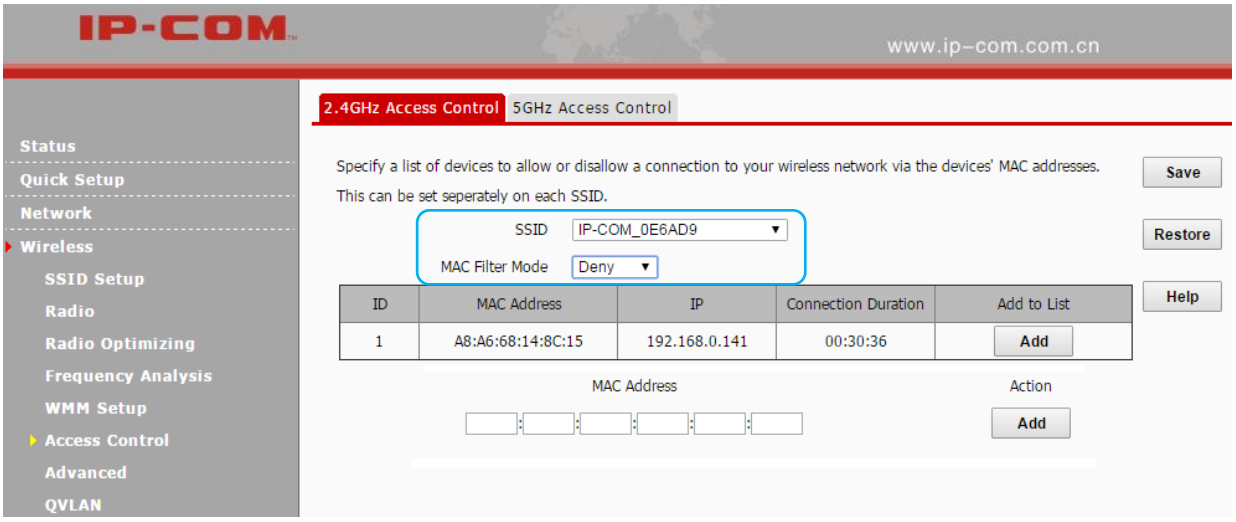
Item	Description
SSID	Select the SSID you wish to configure access control settings.
MAC Filter Mode	Configure the MAC filter mode. • Disable: Disable the Access Control feature. • Allow: Only MAC addresses in the access control list are allowed to connect to the SSID. • Deny: Only MAC addresses in the access control list are not allowed to connect to the SSID.

On this page, you can also view wireless clients currently connected to the selected SSID so that you can quickly add the MAC address you wish to configure access control settings.



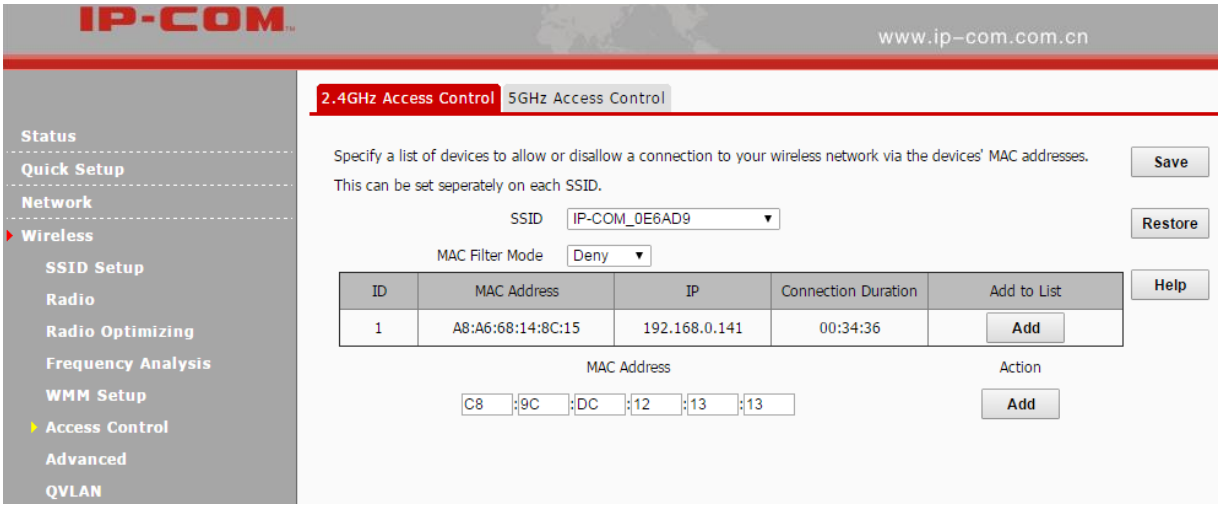
To only deny the computer at the MAC address of the C8:9C:DC:12:13:13 to join your SSID IP-COM_0E6AD9:

1. Select the SSID **IP-COM_0E6AD9** and set the MAC filter mode to **Deny**.

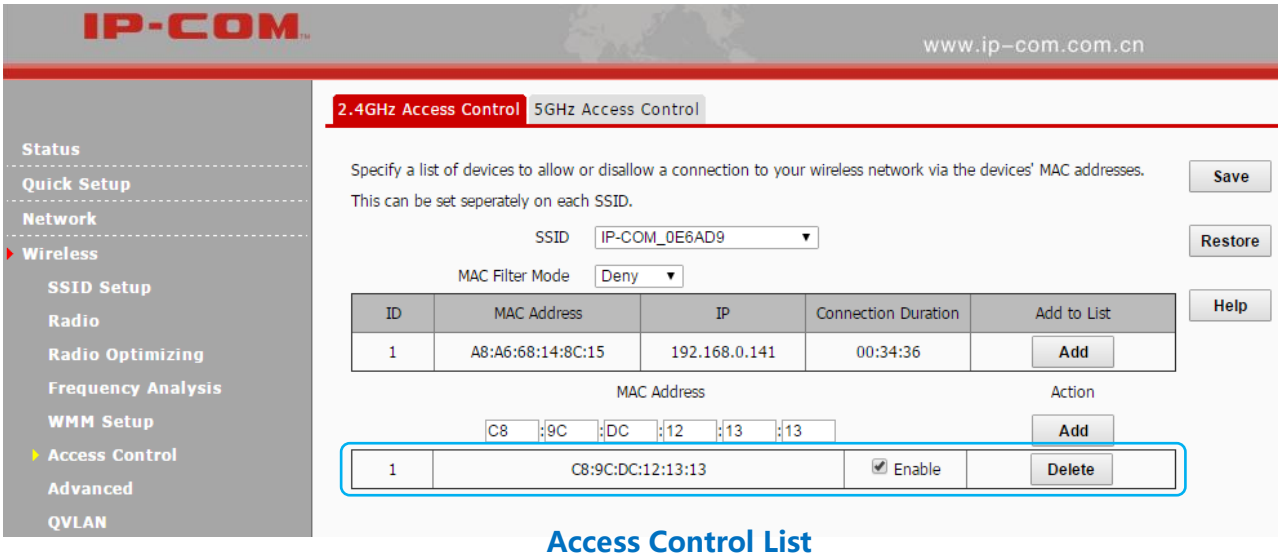


2. Enter C8:9C:DC:12:13:13 in the MAC Address field and click **Add**.

If the MAC address you want to configure has been in the client list, directly click **Add**.



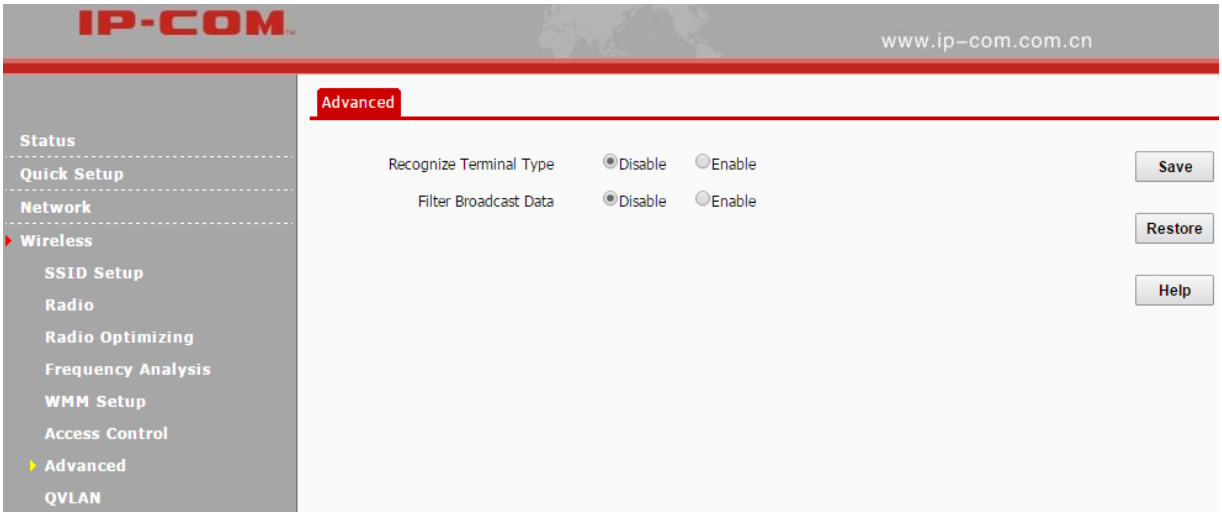
3. Click **Save** to apply your settings.



Access Control List

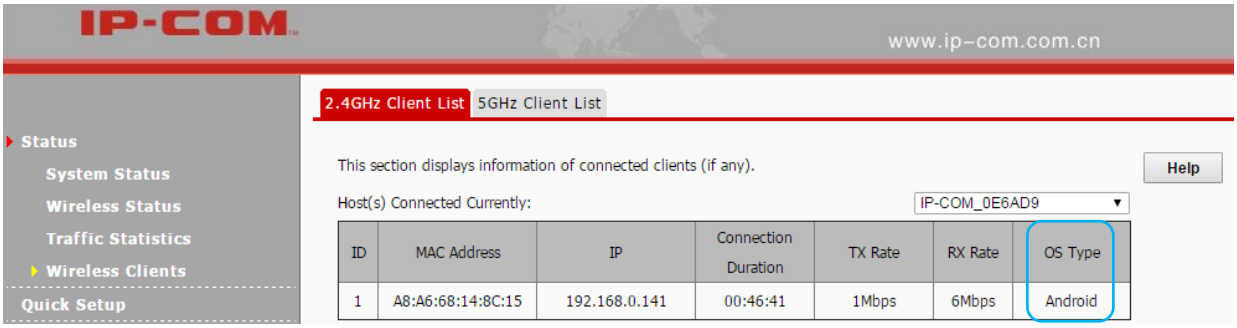
3.4.7 Advanced

This section allows you to recognize terminal types and filter broadcast data. Click **Wireless** > **Advanced** to enter page below:



Recognize Terminal Type

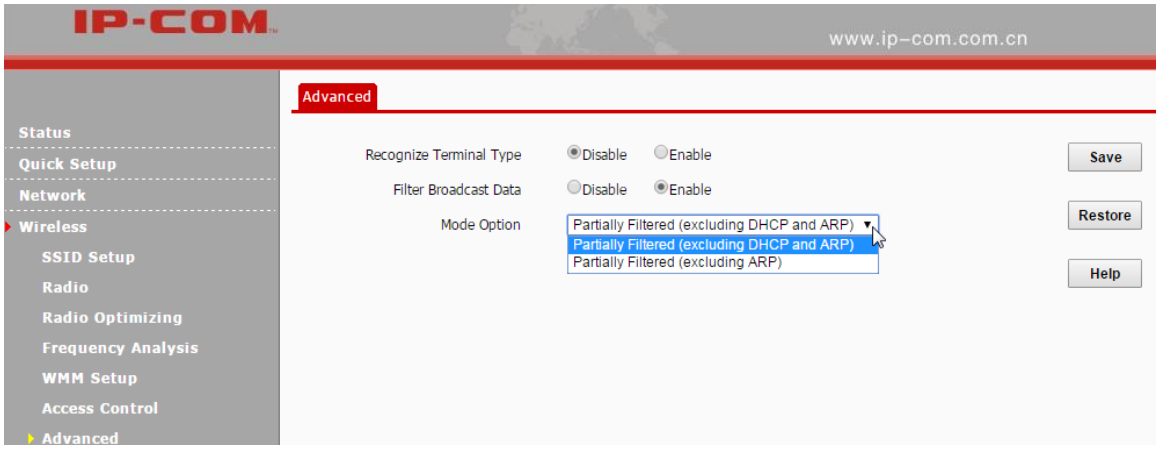
When this feature is enabled, the AP will be able to recognize the terminal type, which makes your network management more efficient. Then click **Status** > **Wireless Clients** to view the terminal type.



Filter Broadcast Data

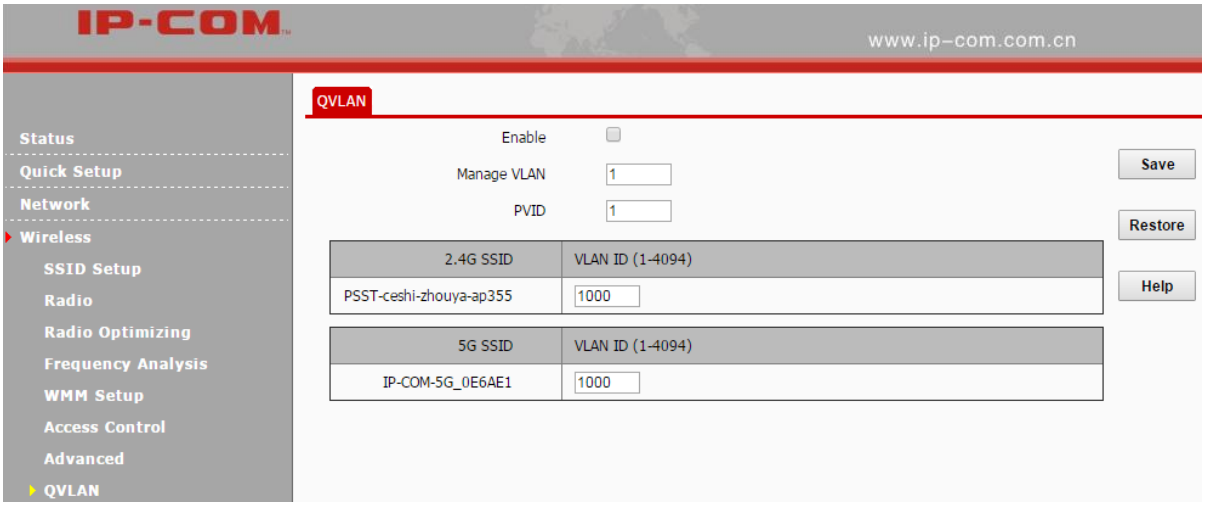
As a main method for discovering unknown devices, broadcast plays an important role in networking. With the

increase of computers in networking, broadcast packets increase and the network is occupied by large numbers of broadcast packets. Thus, the networking transmission capacity will be reduced greatly. This feature helps to filter broadcast packets, avoiding broadcast storm effectively.



3.4.8 QVLAN

When using this feature, users could also assign different VLAN IDs to different wireless networks, which makes it possible to get it work with switches which as VLAN assigned for different access levels and authorities. Click **Wireless > QVLAN** to enter page below:



Parameters Description:

Item	Description
Enable	Check it to enable the QVLAN feature. It is disabled by default.
Manage VLAN	802.1Q manage VLAN ID of the AP. The default value is 1. Once the manage VLAN is changed, you need to re-connect to the new manage VLAN to manage the AP.
PVID	Belonging VLAN ID of the LAN port of the AP. The default is 1. Once QVLAN is enabled, the LAN port of the AP will be the Trunk port.
2.4G SSID	Display SSIDs which have been enabled at 2.4GHz on the AP.

5G SSID	Display SSIDs which have been enabled at 5GHz on the AP.
VLAN ID	Configure the corresponding SSID's VLAN ID. It is 1000 by default. You can specify a value between 1 and 4094. When the VLAN is enabled, wireless port of the SSID can be regarded as an Access port. Its PVID and VLAN ID are the same.

Different data, tagged or untagged, will be processed in different ways, after being received or sent by ports of different link types, which is illustrated in the following table:

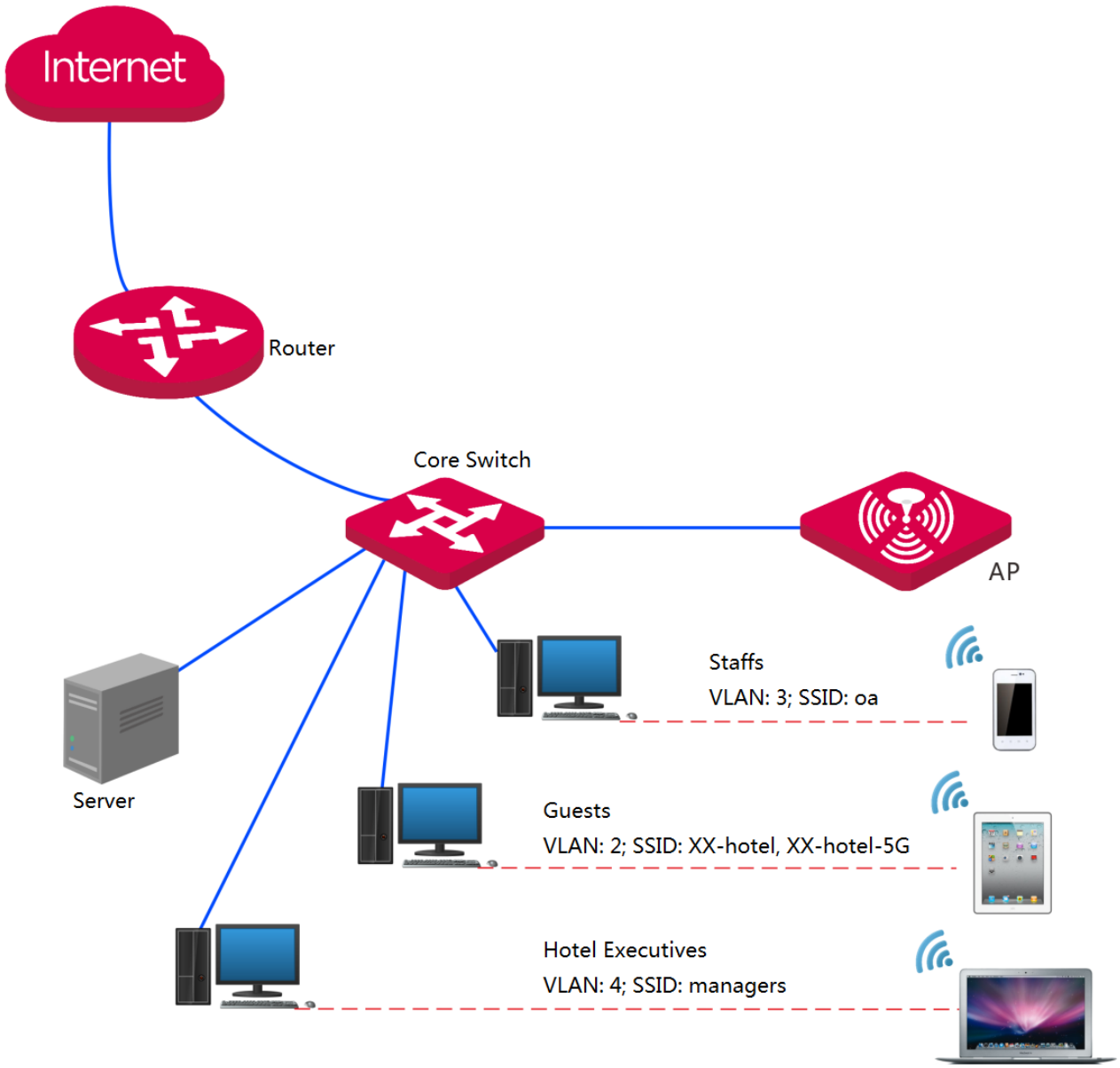
Port Type	**Receiving Packets**		**Sending Packets**
	Receiving Tag Packets	**Receiving Untag Packets**	
Access	Packets will be forwarded to other ports in the corresponding VLAN according to the VID in the Tag.	Data will be forwarded to other ports in the corresponding VLAN according to PVID on this port.	Packets will be sent after removing the VLAN tag.
Trunk			VID ＝ PVID: Packets will be sent after removing the VLAN tag. VID ≠ PVID: Packets will be sent directly.

QVLAN Application Example:

【Requirements】

WiFi needs to be covered in a hotel. People in a hotel are generally classified into three kinds: hotel executives, hotel staffs and guests. Hotel executives can access both the Internet and internal network in the hotel. Hotel staffs can only have the access to internal network in the hotel. Guests can only access the Internet via Ethernet cables or wirelessly.

【Network Topology】



【Solution】

- Divide 802.1 QVLAN on the core switch to isolate hotel executives, hotel staffs and guests.
- IP-COM AP355: Multiple SSIDs and QVLAN settings
- Different SSIDs have different security settings, and different people connect to different SSIDs.
- Three kinds of clients are involved in this example. And up to 12 SSIDs (2.4GHz: 8; 5GHz: 4) can be supported on this AP. Remaining SSIDs will be:

  1） set to SSIDs which will be used by large amounts of clients, like guest and staffs. Verify that these SSIDs' VLAN settings are correct.

  2）disabled.

【Configurations】

1. Divide VLAN on the core switch.

Port Connect to…	VLAN	Port Type	PVID
Guests	2	Access	2
Staffs	3	Access	3
Hotel Executives	4	Access	4
AP	1, 2, 3, 4	Trunk, all VLANs allowed	1
Internal Server	3, 4	Trunk, VLAN3 and VLAN4 allowed	1
Router	2, 4	Trunk, VLAN2 and VLAN4 allowed	1

2. SSIDs and VLANs configured on the AP

Wireless Clients	SSID	VLAN ID
Guests	XX-hotel	VLAN2
Guests	XX-hotel-5G	VLAN2
Staffs	oa	VLAN3
Hotel Executives	managers	VLAN4

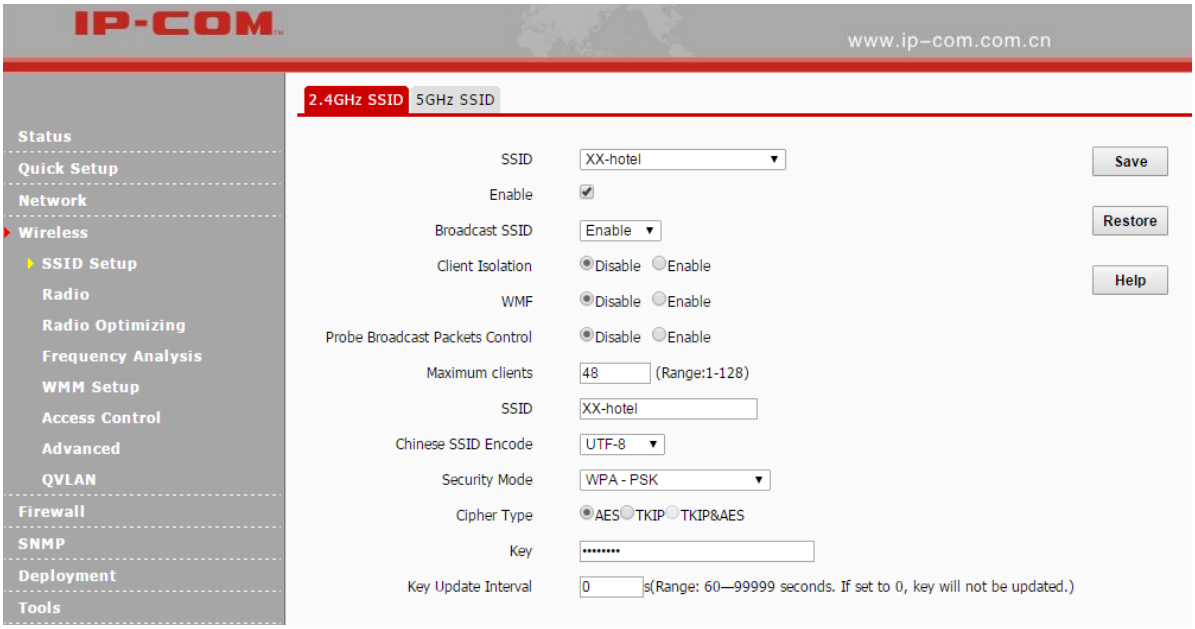
【Configuration Considerations】

To ensure that wireless clients connecting to AP(s) can have normal accesses, QVLAN settings should be supported and configured on the router and on the internal server.

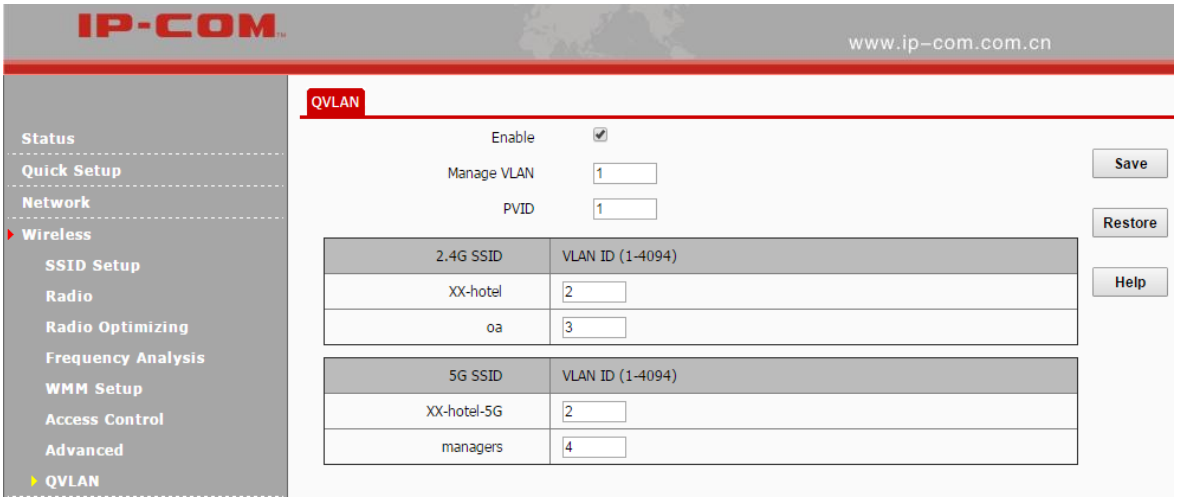
【Configuration steps on this AP】

1. Log in to the Web UI of the AP and click **Wireless > SSID Setup**.

2. Enable 4 SSIDs. In this example, we'll enable 2 SSIDs at 2.4GHz and 2 SSIDs at 5GHz. They will be: XX-hotel, XX-hotel-5G, oa, managers. Make them encrypted and then click **Save**.



3. Click **Wireless** > **QVLAN** to configure QVLAN settings on the AP.



3.5 Firewall

The following parts are included:

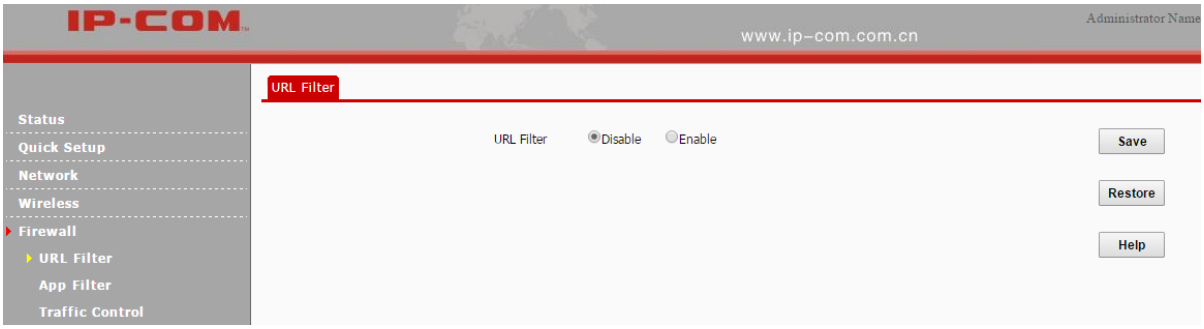
URL Filter: Configure different access rights for different URL categories to rationally manage network access rights.

App Filter: Filter some popular mobile apps, like IM, Video, etc.

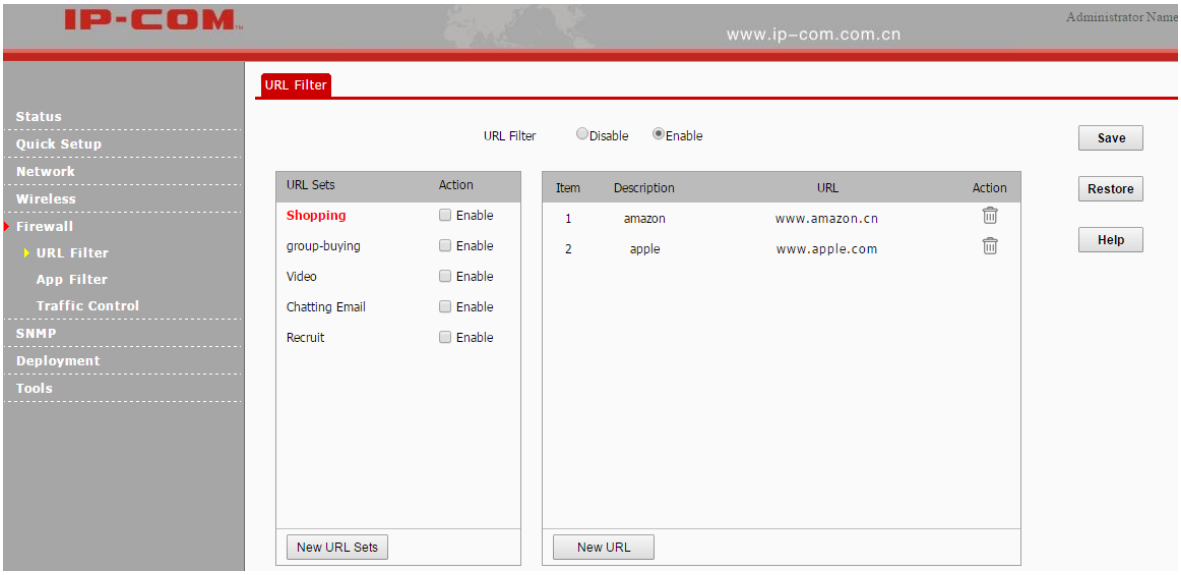
Traffic Control: Configure traffic control rules so that all clients can share network resources properly.

3.5.1 URL Filter

This page allows you to configure access rights for specified URLs, like online shopping, video, etc. By default, this feature is disabled. Click **Firewall** > **URL Filter** to enter page below:

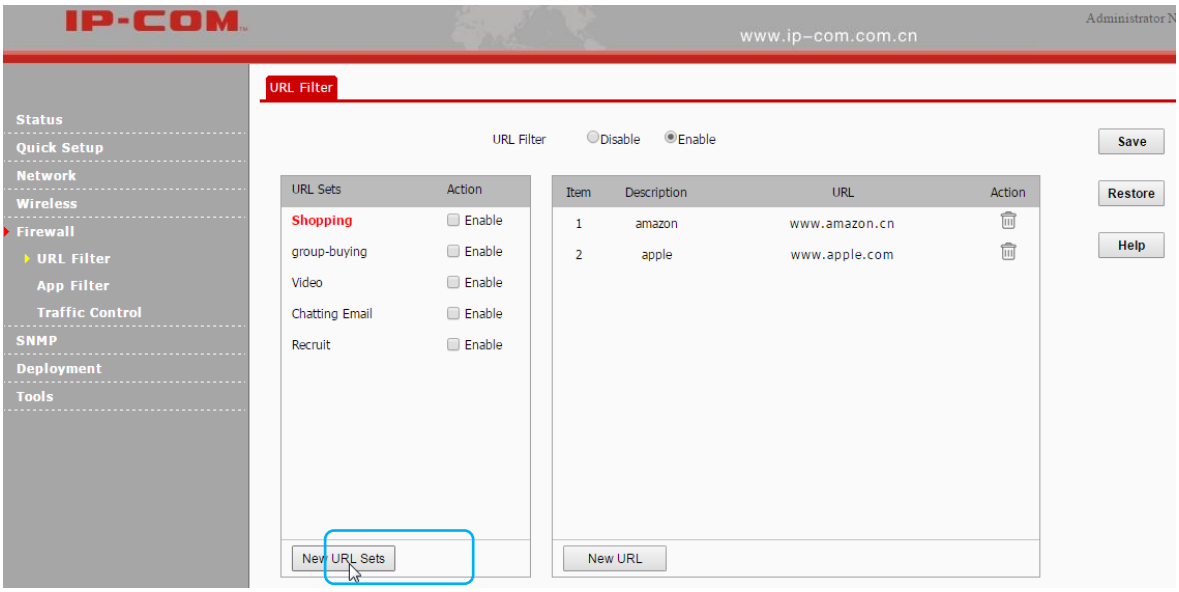


The default 5 URL categories (online shopping, shopping, video, Email and Recruit) can't be deleted. Click URL Category to customize URL info. Up to 10 URL entries can be supported for every URL category. Once some URLs are enabled to be filtered, clients won't be able to access them.

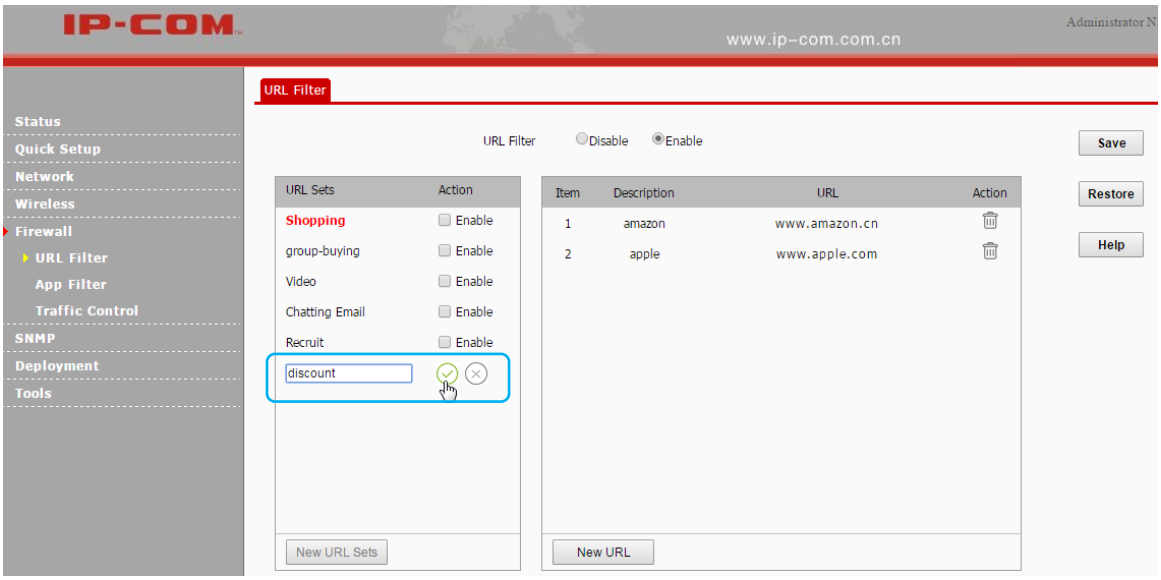


To add a new URL sets:

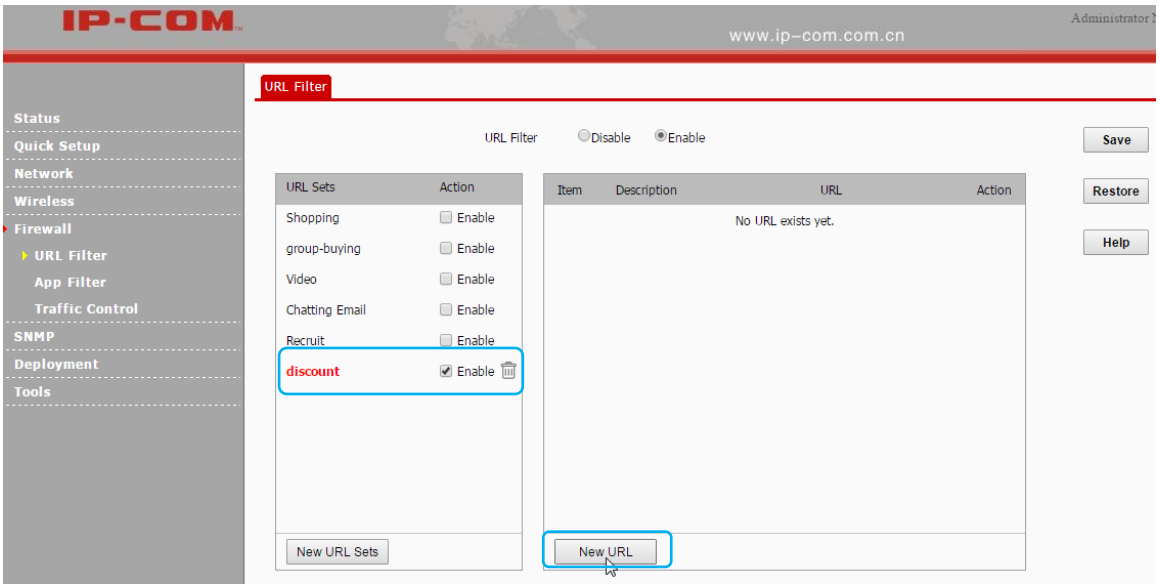
1. Click **New URL Sets**.



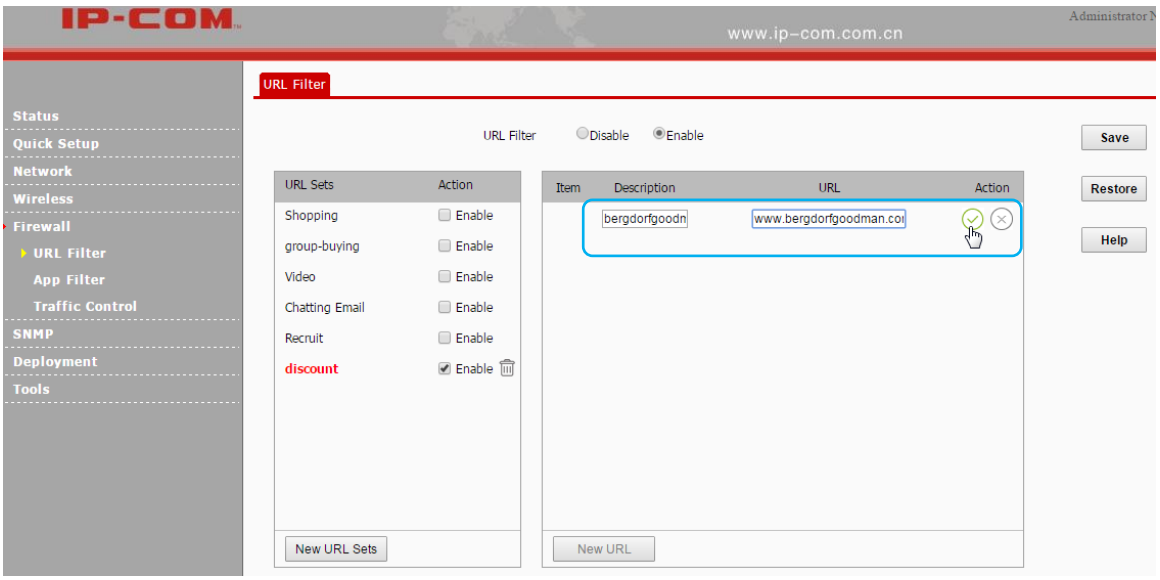
2. Specify the URL set, say, discount, and then click .



3. Click the URL set you've created, and then click **New URL**.

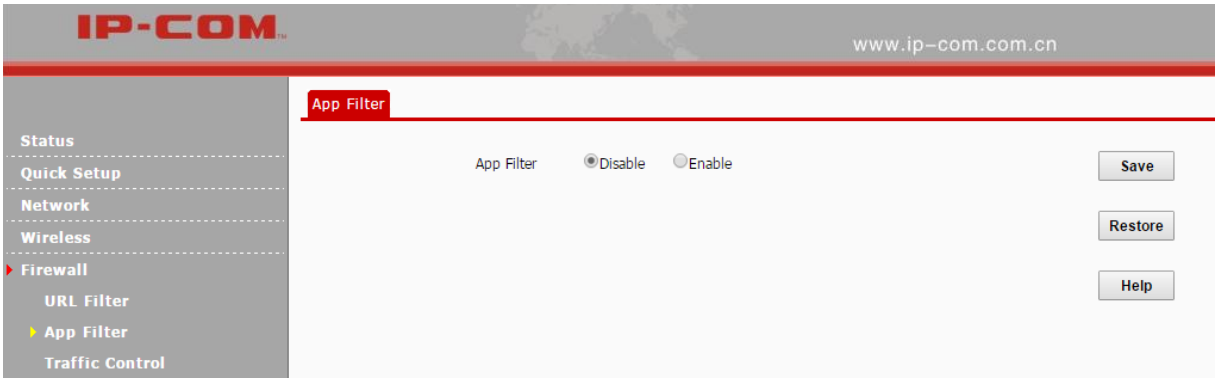


4. Give a description for the URL, specify the URL field, click and then click **Save.**

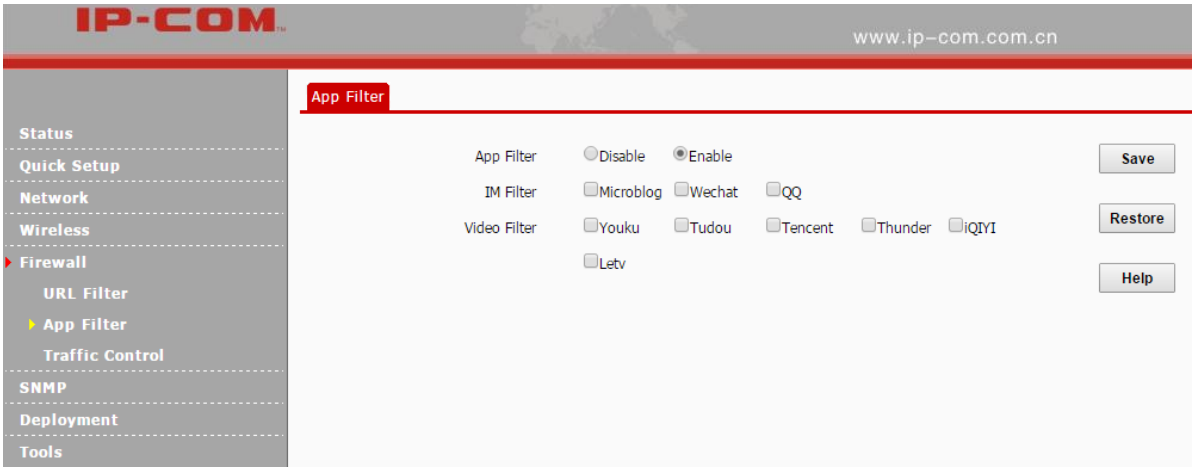


3.5.2 App Filter

This feature allows you to filter some apps, like IM, Video, etc. This feature is disabled by default. Click **Firewall > App Filter** to enter page below:

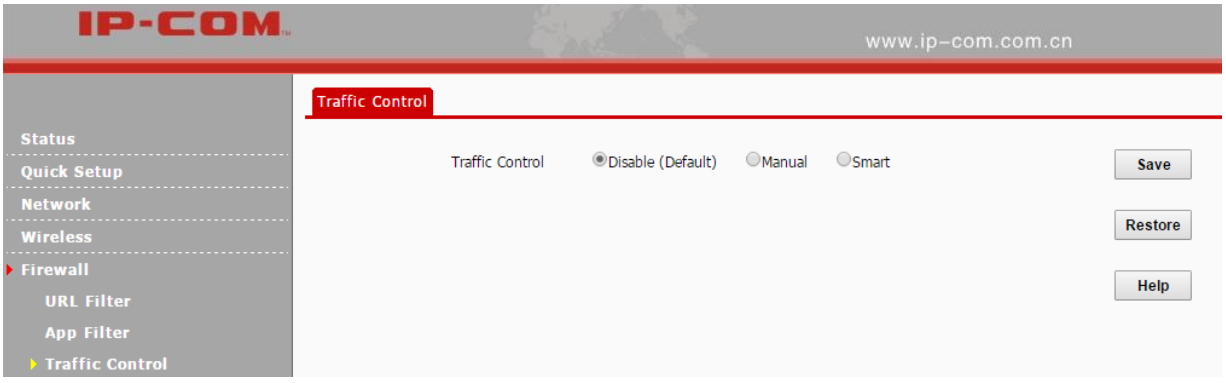


Checking the box before the corresponding app can enable its filtering. Then clients won't be able to use this app.



3.5.3 Traffic Control

Some apps, like P2P download, may consume lots of bandwidth. However, the total bandwidth is limited. If some apps consume too much bandwidth, others' network experience will be affected. To ensure that all users can share network resources properly, you can limit wireless clients' traffic via this feature. It is disabled by default. Click **Firewall > Traffic Control** to enter page below:



The following two traffic control methods are supported on this device:

(1) Manual: Every SSID and every client can only use the pre-configured bandwidth and the actual traffic can't be greater than the set limit.

(2) Smart: Based on the total bandwidth the ISP has provided, all clients dynamically share the AP's total bandwidth on average in case of bandwidth waste.

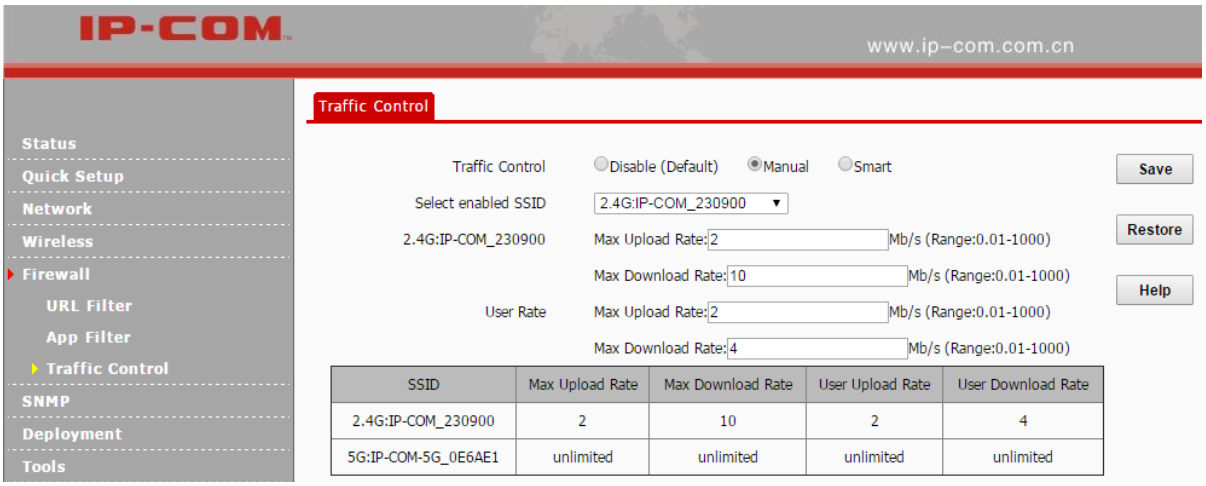
Configuration steps for manual traffic control:

1. Traffic Control: Select **Manual**.

2. Select the SSID you want to configure from the drop-down menu.

3. Set the max upload/download rate for both the SSID and the user.

4. Click **Save** to apply your settings.



Configuration steps for smart traffic control:

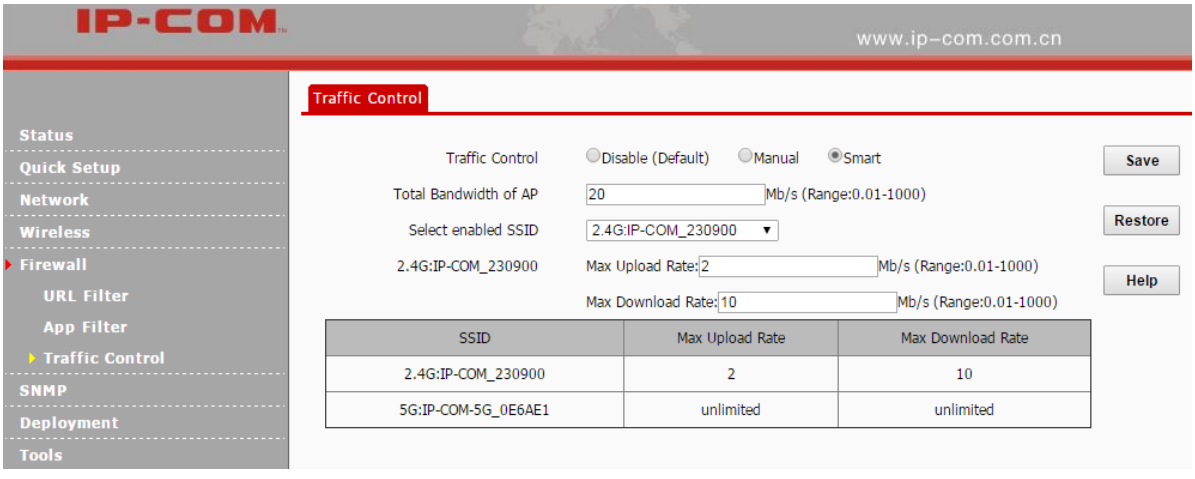
1. Traffic Control: Select **Smart**.

2. Total Bandwidth of AP: Set the total bandwidth the ISP has provided.

3. Select the SSID you want to configure from the drop-down menu.

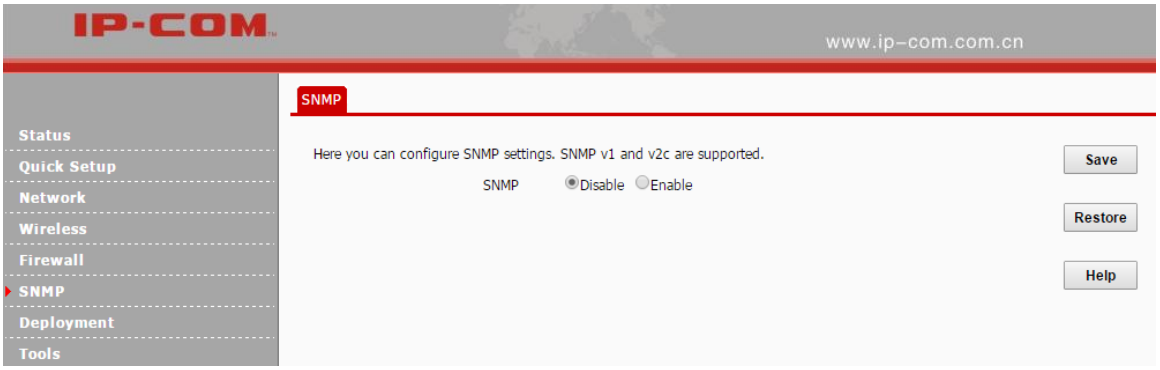
4. Set the max upload/download rate.

5. Click **Save** to apply your settings.

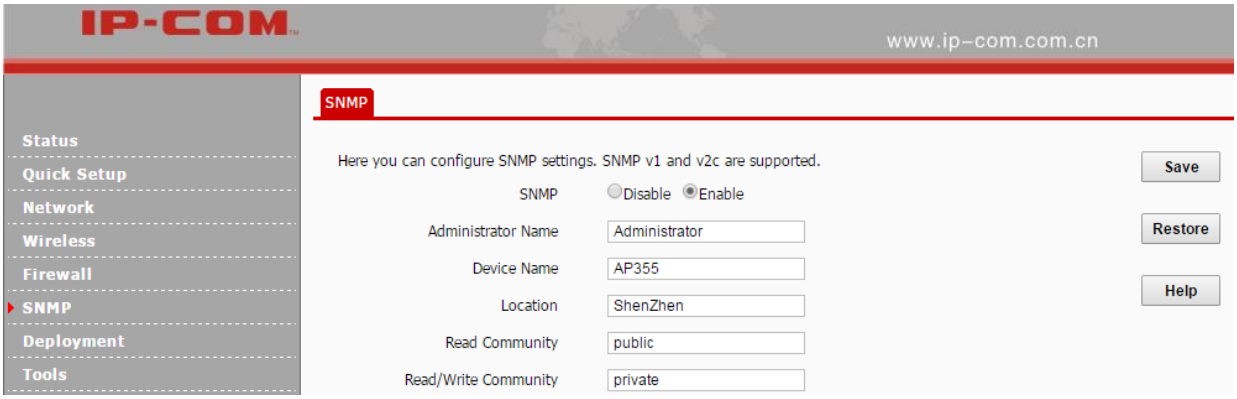


3.6 SNMP

If you want to manage your AP via SNMP, click **SNMP** to enter page below:



By default, SNMP is disabled. Check the **Enable** box to enable SNMP.



Parameters Description:

Item	Description
SNMP	Disable/Enable the SNMP feature. It is disabled by default.
Administrator Name	Administrator name of the AP. It is "Administrator" by default.
Device Name	Device name of the AP. The default name is AP355.
Location	Where the AP is located. The default is Shenzhen.
Read Community	Indicate the community string for read access to permit reading this AP's SNMP information. The default is public.
Read/Write Community	Indicate the community string for write/read access to permit reading and writing this AP's SNMP information. The default is private.

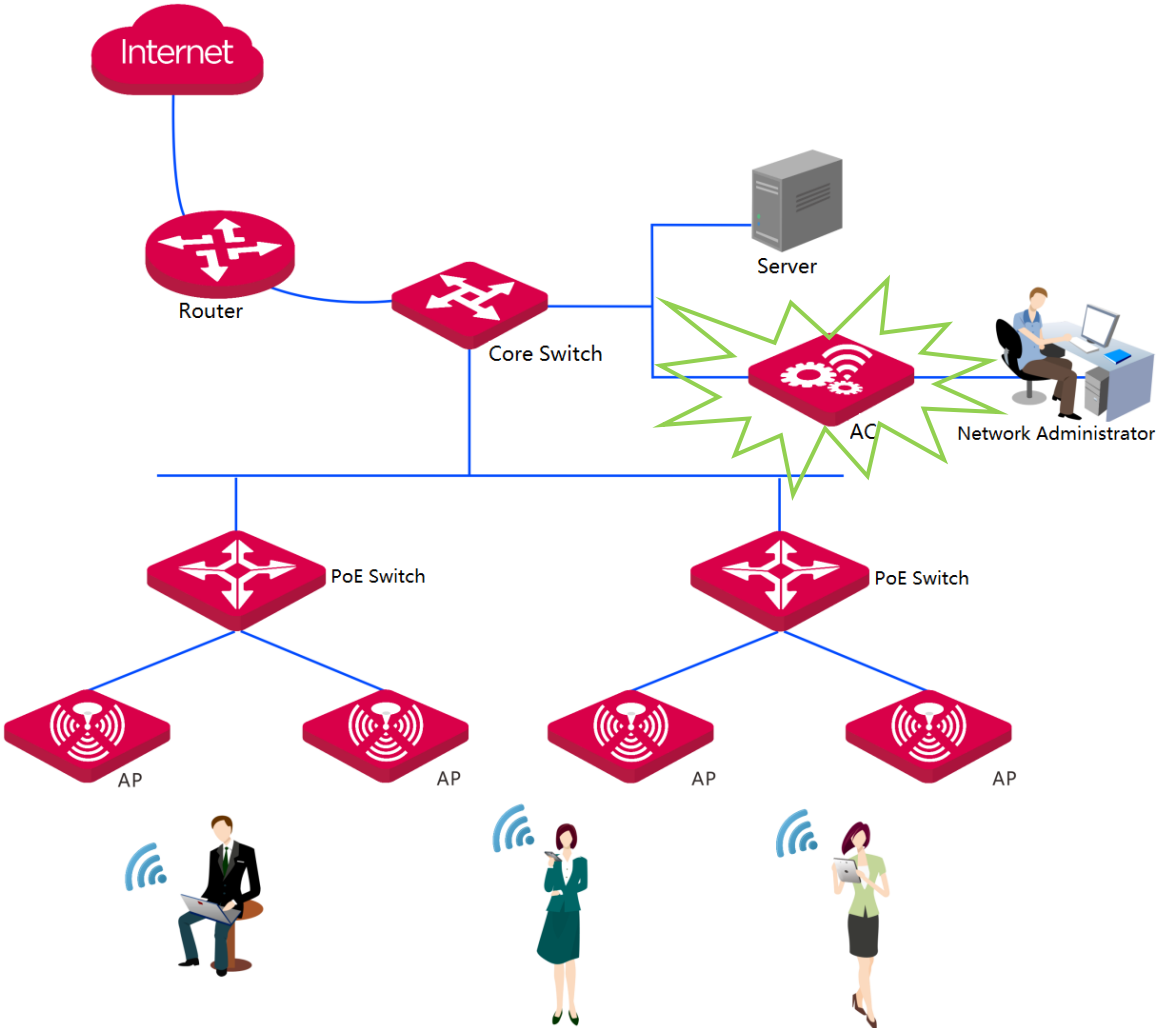
3.7 Deployment

Two deployment modes are supported on this AP: Local and Cloud. If there are many APs deployed in your

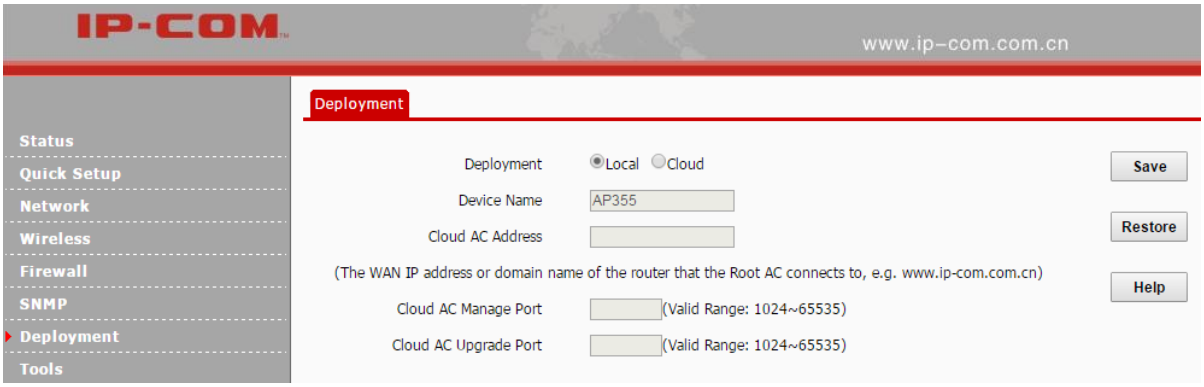
network, it is suggested to use IP-COM access controller AC2000 to centrally manage these APs.

➘ Local

When there are many APs centrally deployed in your network, it is suggested to set these APs in **Local** mode, so that APs can be managed by the local AC (access controller).



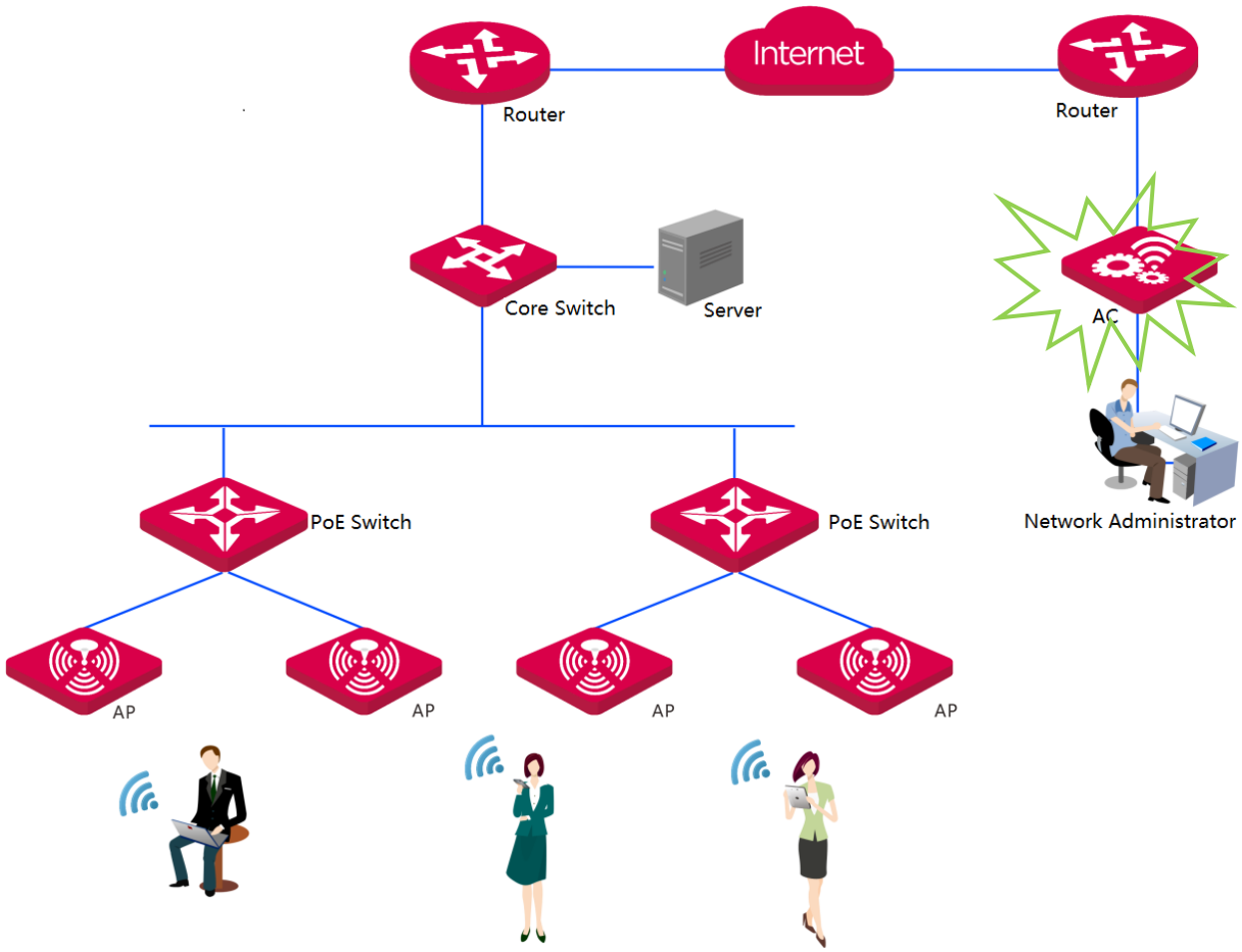
By default, it is in **Local** mode.



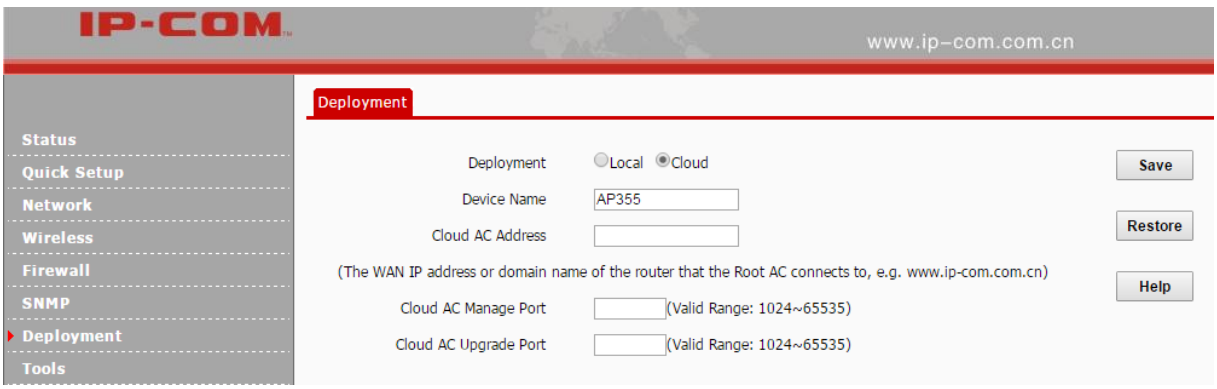
➘ Cloud

When many APs are scattered here and there, it is suggested to set these APs in **Cloud** mode, so that the AC (cloud

AC) from the Internet side can centrally manage these scattered cloud APs.



Go to **Deployment** page, select **Cloud**:



Parameters Description:

Item	Description
Deployment	Configure different deployment modes to manage APs. It is in **Local** mode by default. • Local: When this mode is selected, all current APs can only be managed by the local AC. • Cloud: When this mode is selected, all current APs can only be managed by the cloud AC or a cloud server. Options need to be configured in Cloud mode:
Device Name	Name of the AP. This item is only available in Cloud mode. It will be very convenient for the network administrator to recognize and manage APs if the device name is modified.
Cloud AC Address	The WAN IP address or domain of the router that the cloud AC connects to. This item is only available in Cloud mode.
Cloud AC Manage Port	The port of the router that the cloud AC connects to and that is used for managing cloud APs (Range: 1024~65535). This item is only available in Cloud mode.
Cloud AC Upgrade Port	The port of the router that the cloud AC connects to and that is used for upgrading cloud APs (Range: 1024~65535). This item is only available in Cloud mode.

3.8 Tools

The following nine parts are included in Tools section.

Maintenance: Upgrade the AP's system software.

Time & Date: Configure system time and web idle timeout for the AP.

Logs: View and manage system logs of the AP.

Configuration: Backup and restore your configurations, and reset your AP to its factory defaults.

User Name & Password: Modify login username and password to prevent unauthorized accesses.

Diagnostics: Troubleshoot your AP to quickly find out where the problem is.

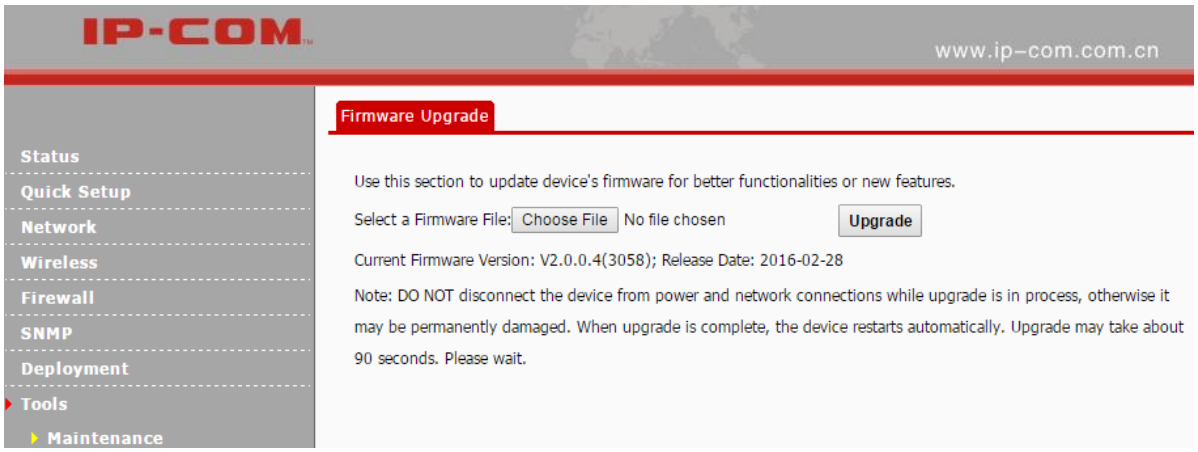
Reboot: Restart your AP.

LED: Turn on/off the LED of the AP.

Uplink Detection: Used for uplink detection.

3.8.1 Maintenance

If your device is in normal operation, it is not advisable to upgrade your device. If you want to acquire the latest software version or better value-added functions for your device, you can access our official website http://www.ip-com.com.cn to download the latest software for upgrading. Click **Tools** > **Maintenance** to enter page below:



Note

Do not disconnect power supply of the AP. If the power supply is interrupted, the upload may fail and you need to re-upgrade it. If you are unable to log in to its web UI after cutting off its power supply during the upgrading, cousult our technical stuff for assitance.

Upgrading Steps:

1. Launch a web browser and go to http://www.ip-com.com.cn to download the latest firmware.

2. Go to the Maintenance page.

3. Click **Choose File** (in Google browser) to locate and select the upgrade file in the corresponding directory on your hard disk.

4. Click **Upgrade** and then follow onscreen instructions to finish the upgrade.

When the upgrading completes, view the current firmware version to judge that whether you've upgraded your AP successfully or not.

3.8.2 Time & Date

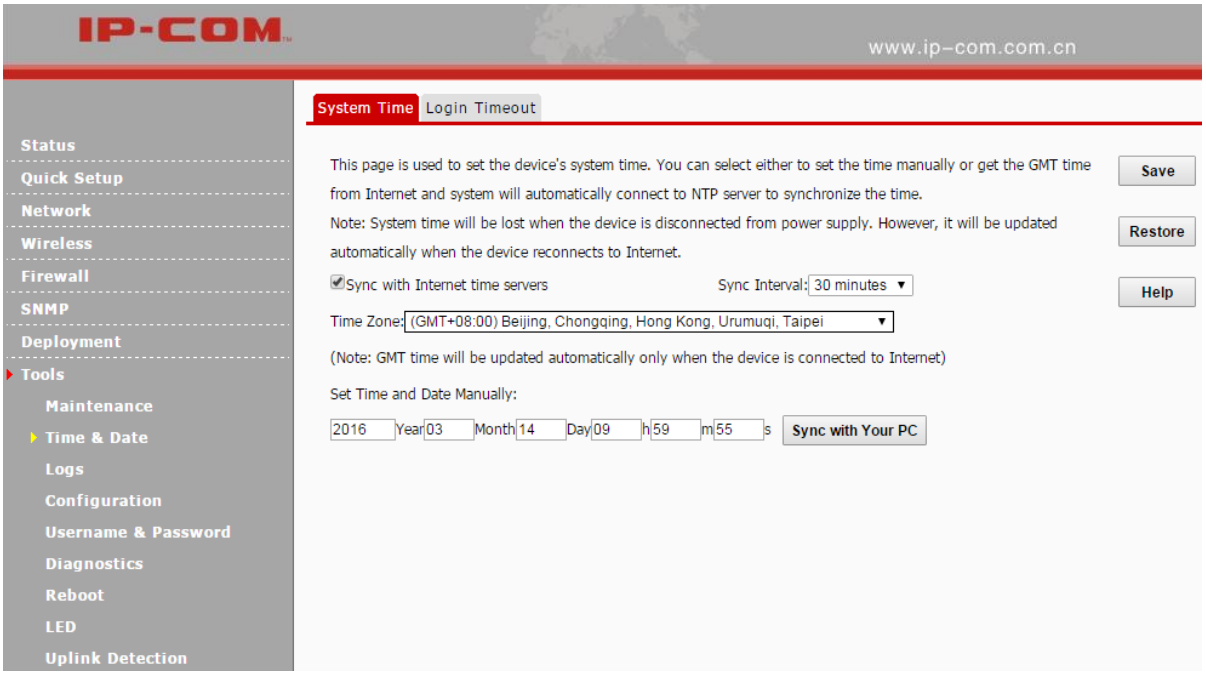
This page allows you to configure the AP's system time and web login timeout.

System Time

Click **Tools > Time & Date > System Time** to enter page below. This page is used to set the device's system time.

Tip

Once power is not delivered on this device, the time settings will be lost. By default, Sync with Internet time servers is enabled. When the device is able to access the Internet, it will automatically connect to the NTP server on the Internet to synchronize the time.



System time can be configured using the following 2 methods:

➘ Sync with Internet time servers

If enabled, system automatically connects to NTP server on the Internet to synchronize the time. To enable this feature, please verify that your AP has connected to the Internet successfully. Method: go to LAN Setup page to configure its IP info.

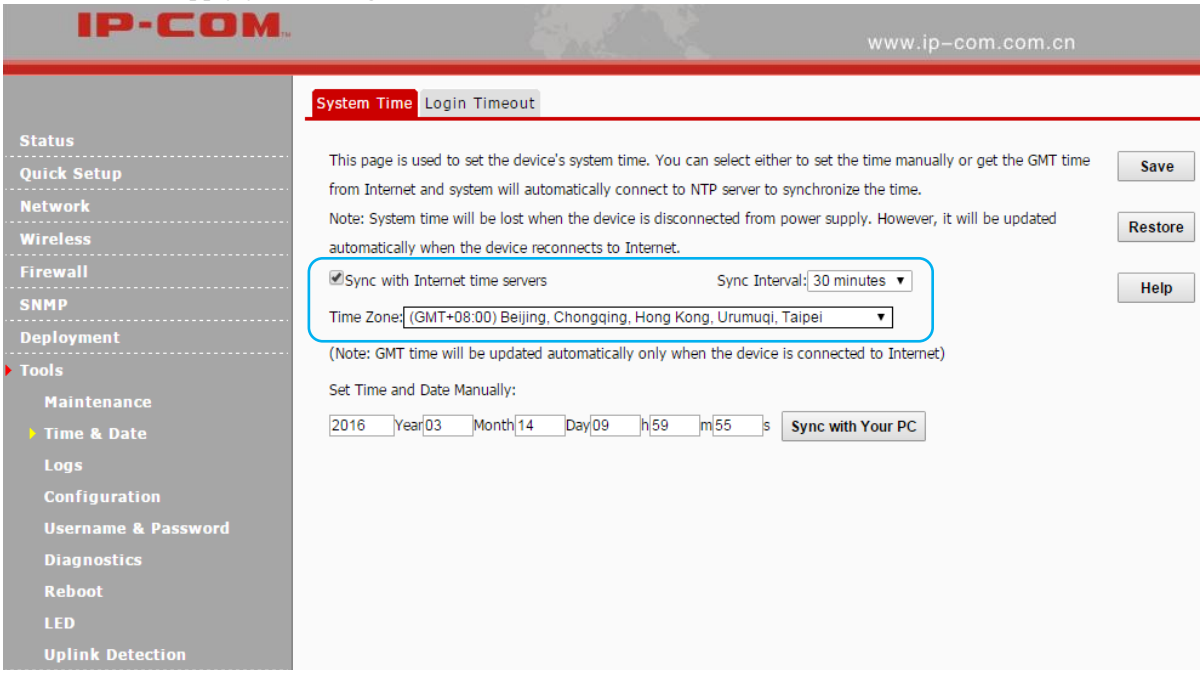
Configuration Steps:

1. Check the **Sync with Internet time servers** box.

2. Select the sync interval, say, 30 minutes.

3. Select your time zone.

4. Click **Save** to apply your settings.



➘ Set Time and Date Manually

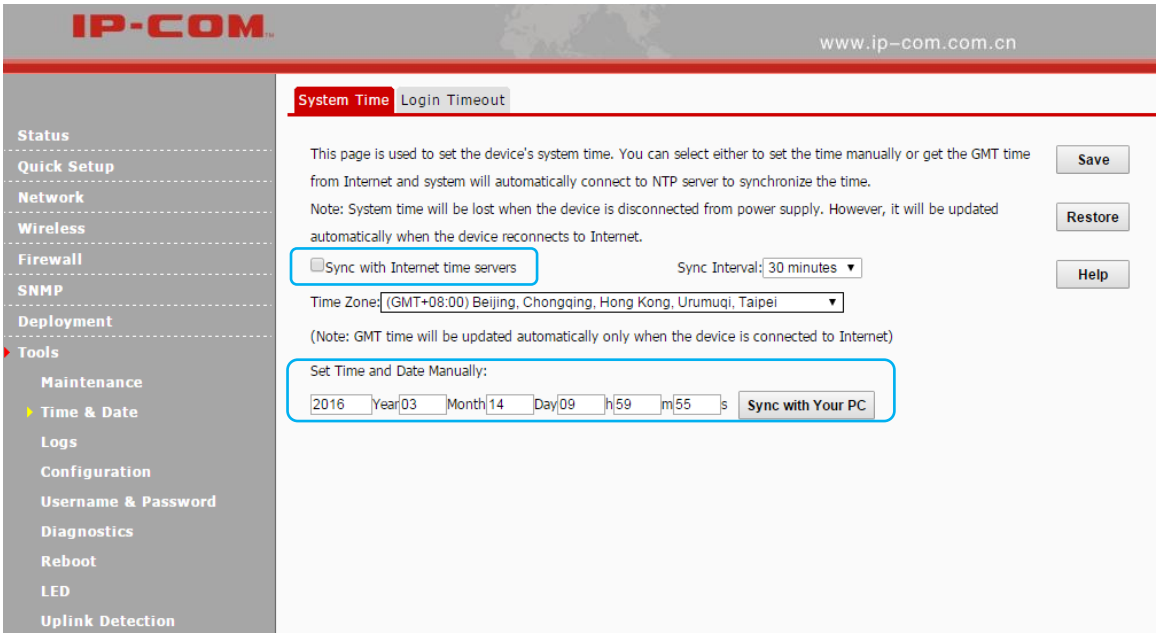
Specify the time and date manually or click **Sync with Your PC** to automatically copy your current PC's time to the device.

Configuration Steps:

1. Uncheck the **Sync with Internet time servers** box.

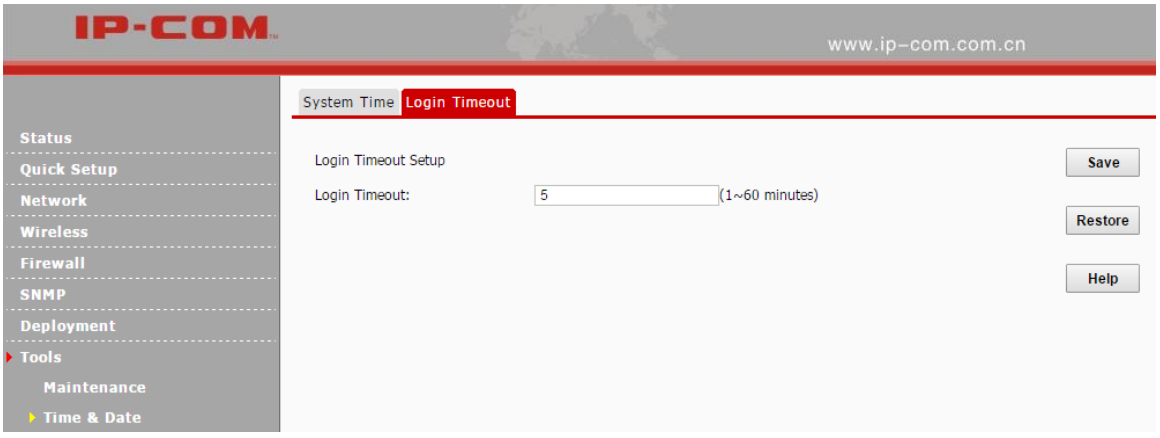
2. Click **Sync with your PC** or enter the correct date and time in the input fields.

3. Click **Save** to apply your settings.



Login Timeout

You are automatically logged out of the web UI after a period of inactivity. You can set the length of the inactive period. The default login timeout is 5 minutes. To change the login timeout, click **Tools > Time & Date > Login Timeout** to enter page below:



3.8.3 Logs

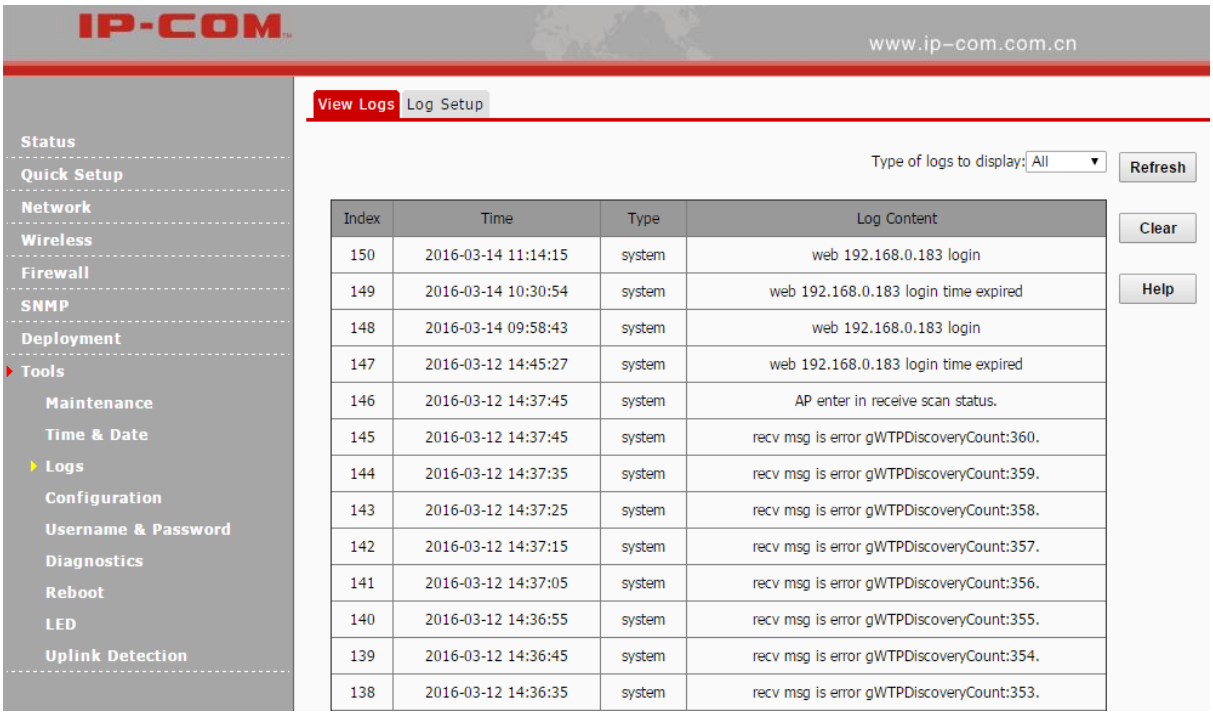
The following two parts are included:

View Logs: View system logs since the latest reboot.

Log Setup: Configure log server and how many logs can be displayed on each page.

View Logs

Click **Tools > Logs > View Logs** to enter page below. Here you can view the history of the device's actions. Two types of logs are supported on this device: All and System. You can select any one of them from the drop-down list. Click **Refresh** to update current log info or click **Clear** to clear all logs.

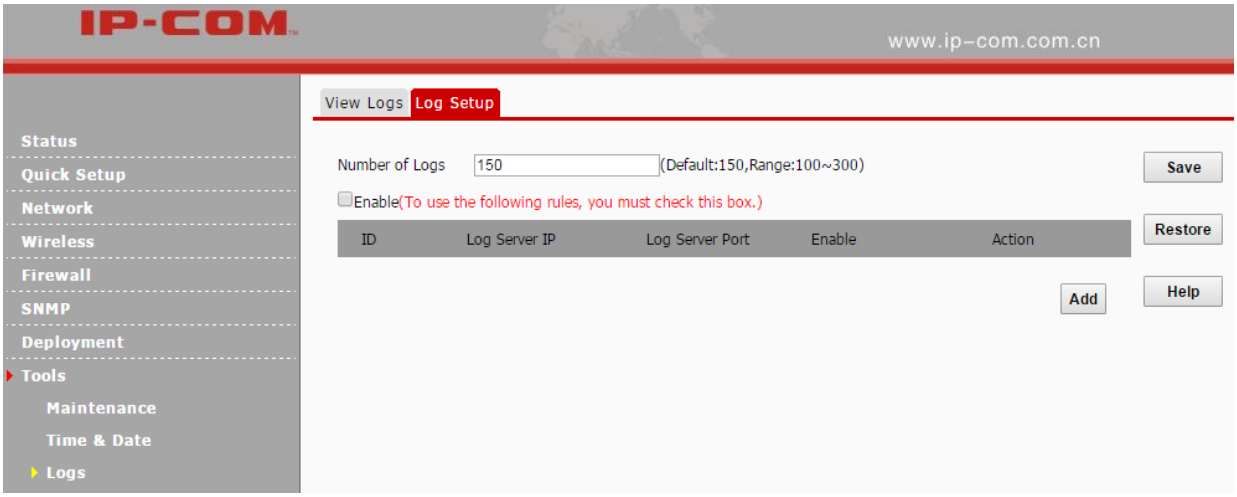


Note

- Rebooting your AP will clear all your system logs.
- Configuring QVLAN settings, powering off your AP, backing up and restoring configurations, resetting and upgrading your AP will reboot your AP.
- To verify that the logs are correctly recorded, go to **Tools > Time & Date** to make your system time correct.

Log Setup

Click **Tools > Logs > Log Setup** to configure system logs. Here you can set up the number of logs and rules of log settings.



➘ Number of Logs

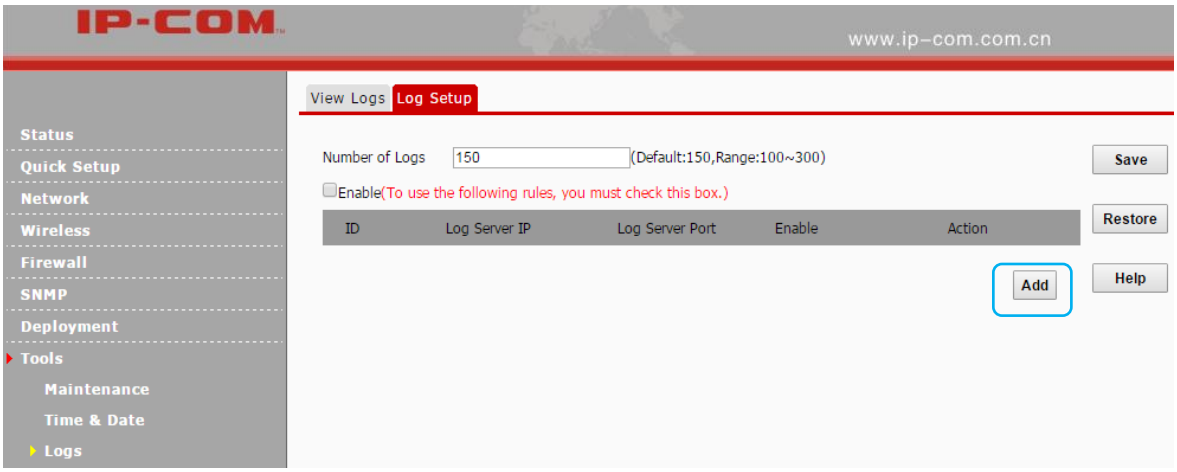
Up to 300 entries can be logged. The default is 150.

➘ Log Server

If configured successfully, the system will begin to log events and simultaneously send them to the specified log server in your LAN. You can view all logs there.

Configuration Steps:

1. Click **Add**.

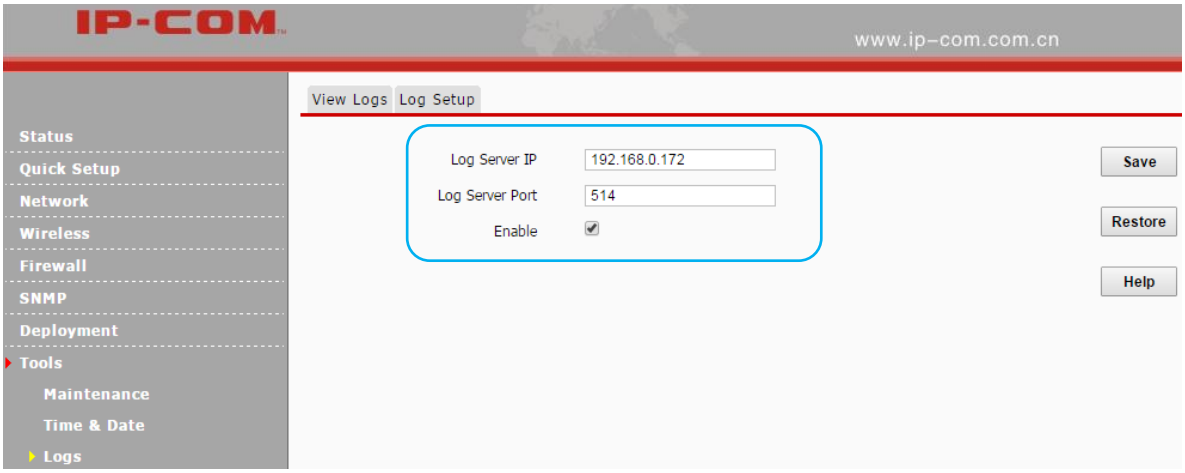


2. Log Server IP: Specify the IP address of the syslog server in your LAN, say, 192.168.0.172.

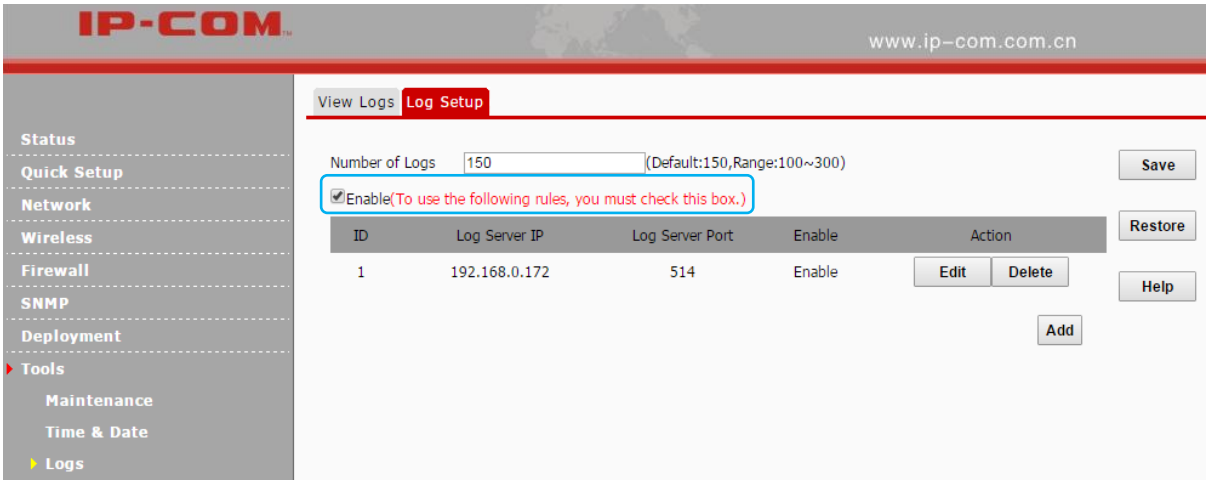
3. Log Server Port: Specify the port of the syslog server in your LAN (If not allowed to configure a port on your server, enter the default value 514).

4. Check the **Enable** box to enable the log server.

5. Click **Save** to apply your settings.



6. Check the "To use the following rules, you must check this box." Option to activate your settings and then click **Save**.



Note

To make sure that system logs can be sent to the server successfully, you need to go to **Network > LAN Setup** to set your AP's IP address, subnet mask and gateway so that the route between the AP and the log serve is reachable.

3.8.4 Configuration

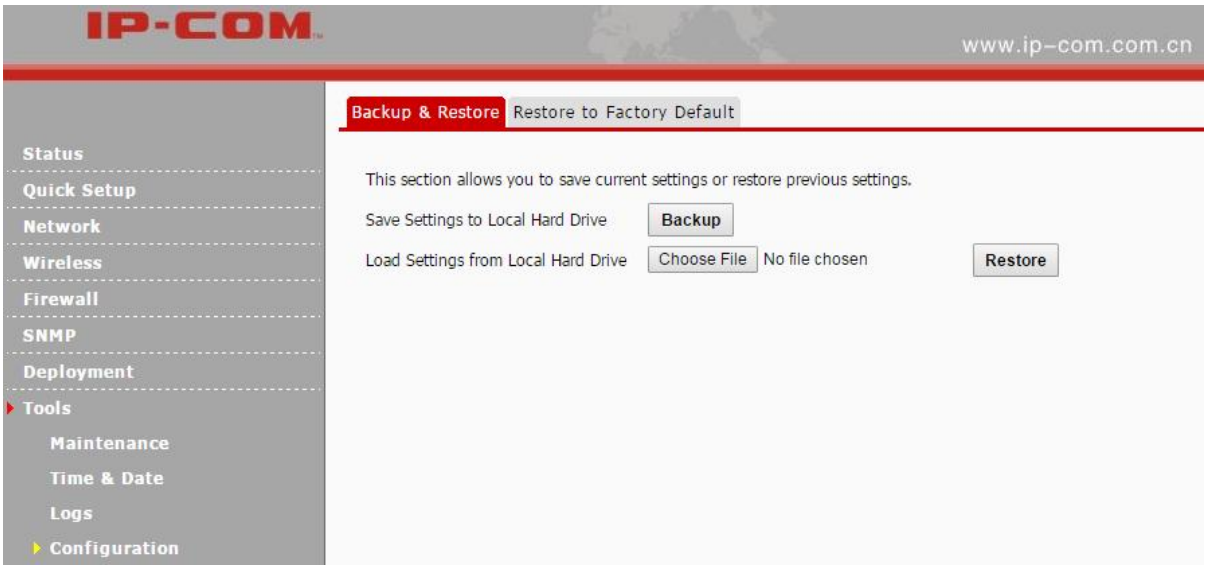
The following two parts are included:

Backup & Restore: Backup current configurations to your local PC and restore previous configurations to your AP.

Restore to Factory Default: Restore your AP to its factory defaults.

Backup & Restore

Click **Tools > Configuration** to enter page below:



➘ **Backup**

If you configure many settings on this device, which will make this device work in good status, it's suggested to backup settings, which will be convenient for troubleshooting and saving time for next time's configuration.

Method: Click **Backup** and then follow onscreen prompts.

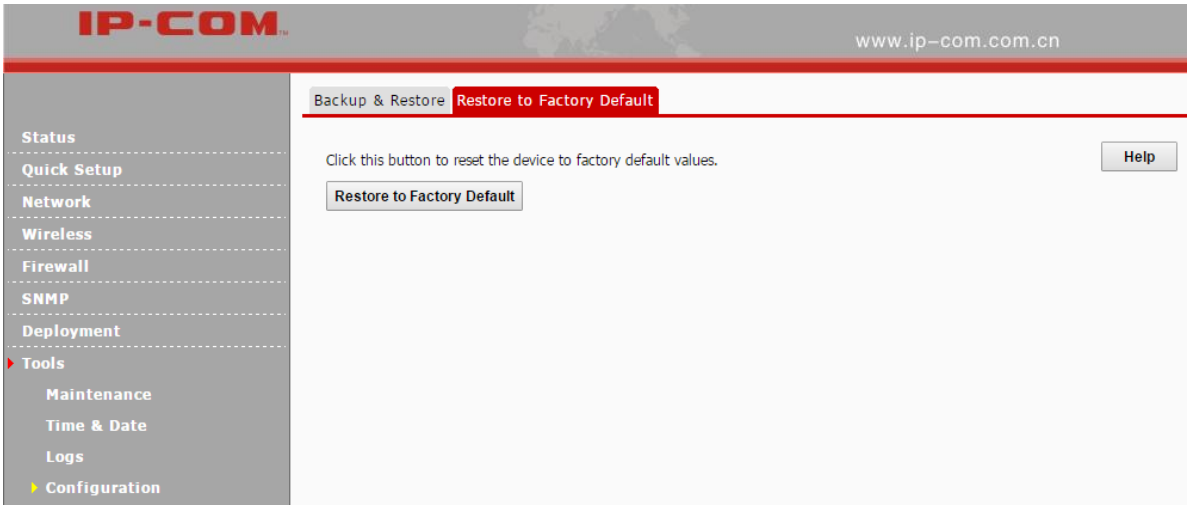
➘ **Restore**

If you need to configure the same settings for multiple APs, or if your AP works improperly, you can restore your AP to its previous configurations which you've backed up.

Method: Click **Choose File** (in Google browser) to download your previous configurations, click **Restore** and then follow onscreen prompts.

Restore to Factory Default

If the device or client connected to the device fails to access the Internet due to incorrect configurations and you cannot solve the problem, click **Tools > Configuration > Restore to Factory Default** to reset the device and then reconfigure it.



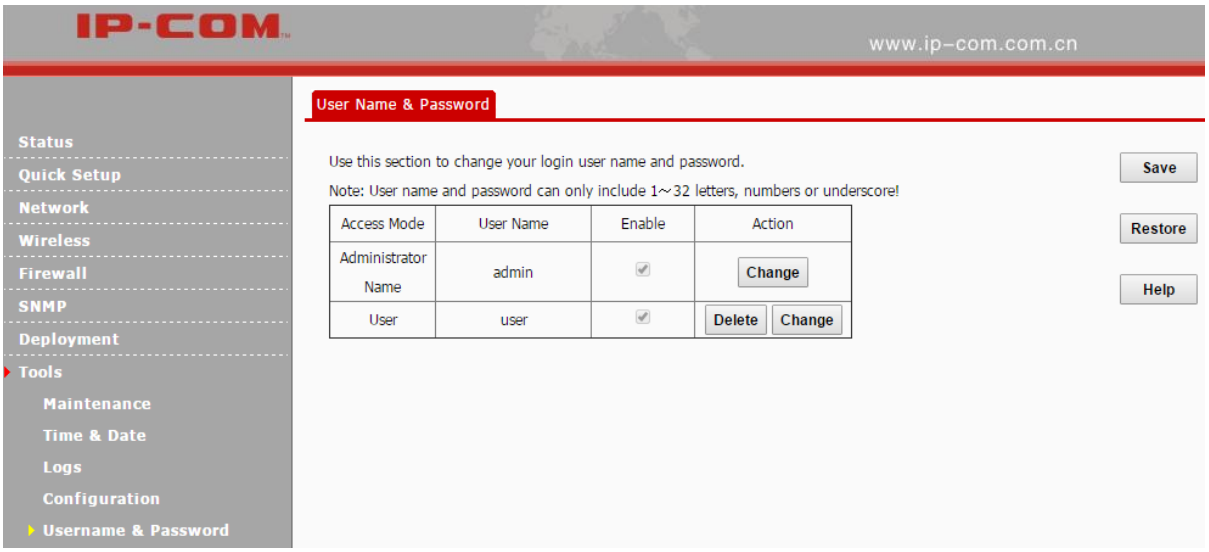
If you forgot the login info of the AP, like login IP address or login username, you can press and hold the **RESET** button with something like a needle for at least 7 seconds to reset your AP.

Tip

After resetting your AP, the login IP address of the AP is 192.168.0.254, and the login username and password are admin for both. For other default settings, see Appendix 2 Default Settings.

3.8.5 User Name & Password

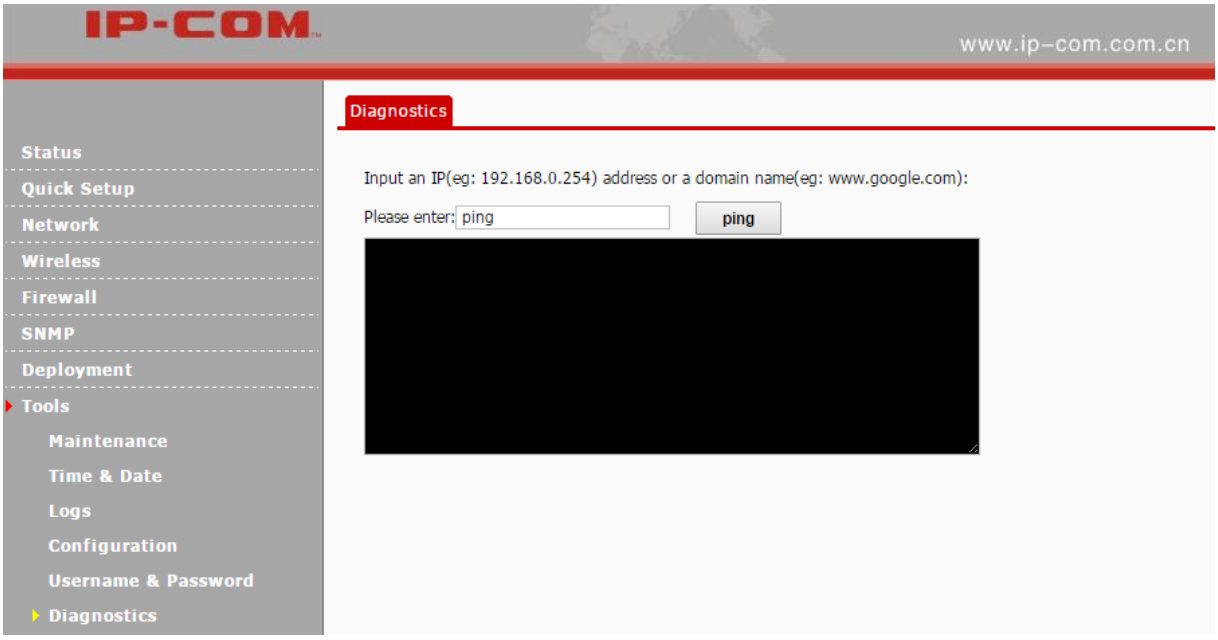
Click **Tools > User Name & Password** to enter page below. Here you can change the user name and password for web login. We suggest that you change this password to a more secure one.



By default, two accounts are supported: administrator and user. The administrator can manage your AP, while the user can only view the AP's relevant information. Both the user name and password for the administrator are **admin**. Both the user name and password for the user are **user**.

3.8.6 Diagnostics

This page allows you to test your network connection. If your network is malfunctioning, click **Tools > Diagnostics** to use the ping utility to test your network and find out where the problem is.



3.8.7 Reboot

When some settings you have configured cannot be activated or your device is functioning improperly, please

reboot your device. The following two parts are included:

Reboot: Reboot your AP manually.

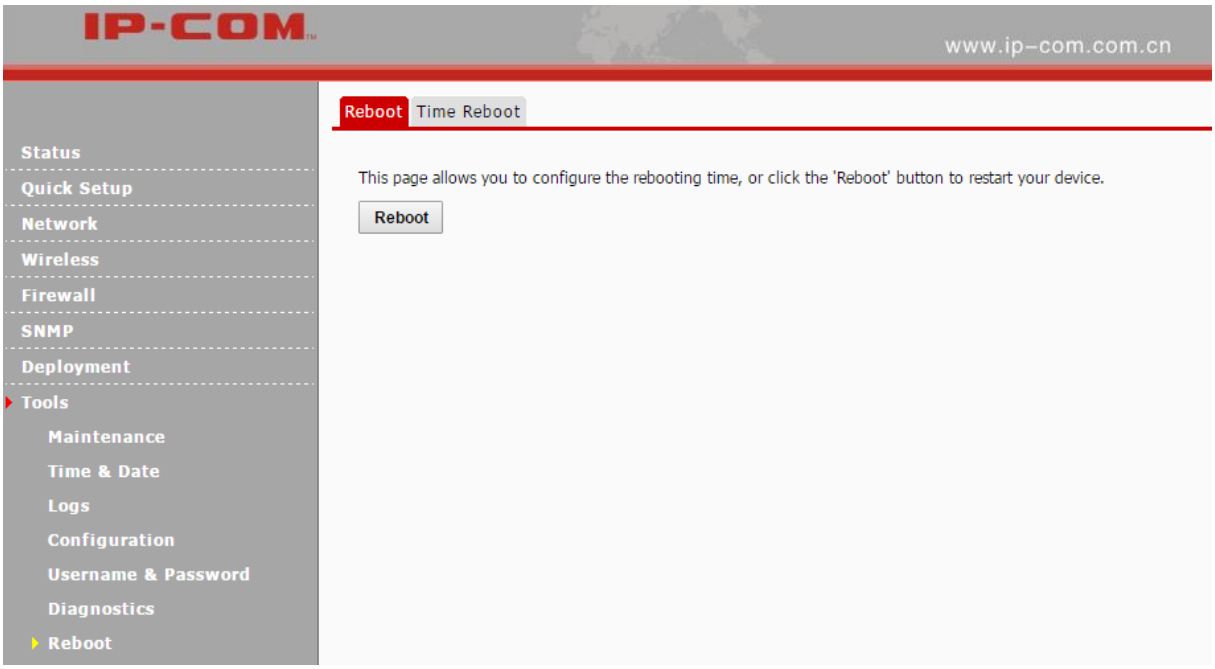
Time Reboot: Reboot your AP at the specified time.

Tip

While rebooting your AP, all your WiFi connections will be disconnected. Thus, please reboot your AP when the network is not busy.

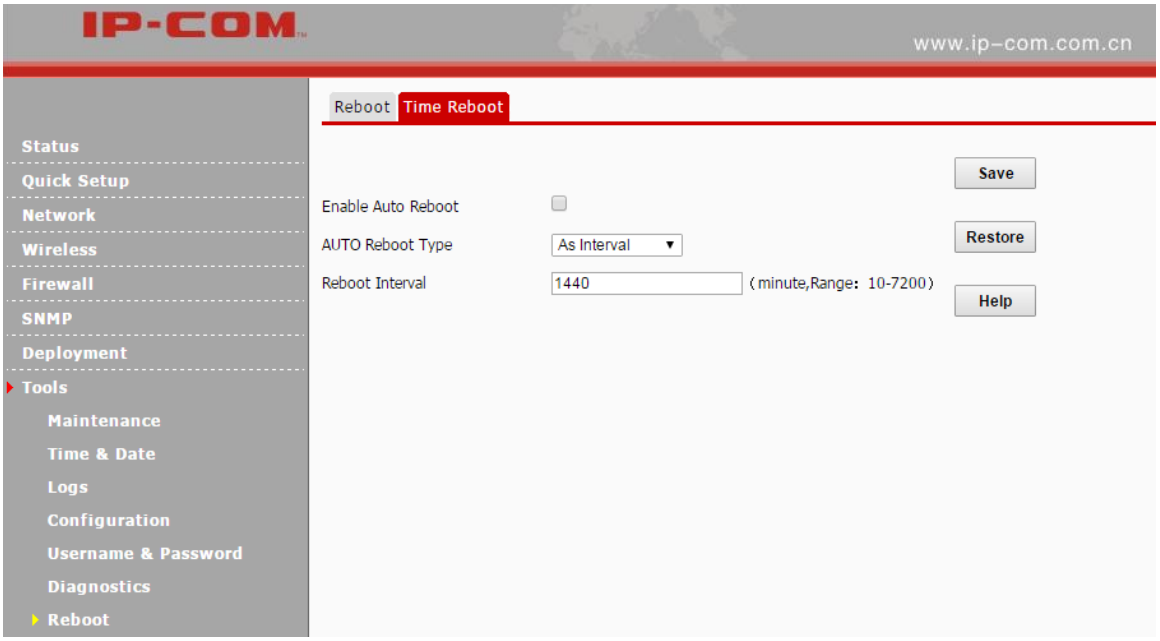
Reboot

Click **Tools > Reboot** to reboot your AP manually.



Time Reboot

Click **Tools > Reboot > Time Reboot** to enter page below. Here you can reboot your device at the specified time. Once this feature is enabled, please make sure that your device is synchronized with the Internet time server.



Two methods for time reboot are available: As Interval and As Scheduled.

➘ **As Interval**

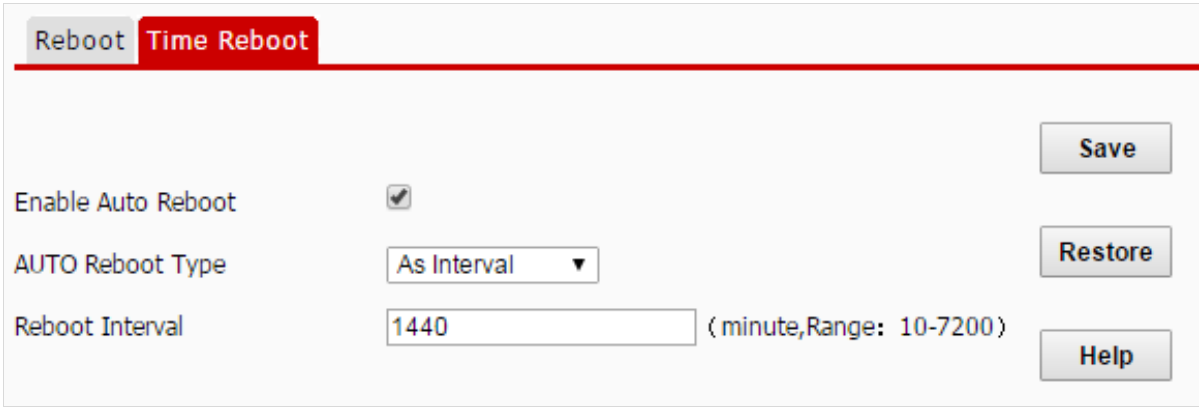
The device will reboot automatically at intervals according to the interval you've configured.

1. Check the **Enable Auto Reboot** Box.

2. Select **As Interval** from the drop-down list.

3. Specify the reboot interval (Recommended: 1440 minutes).

4. Click **Save** to apply your settings.



➘ **As Scheduled**

The device will reboot regularly according to the time you've configured.

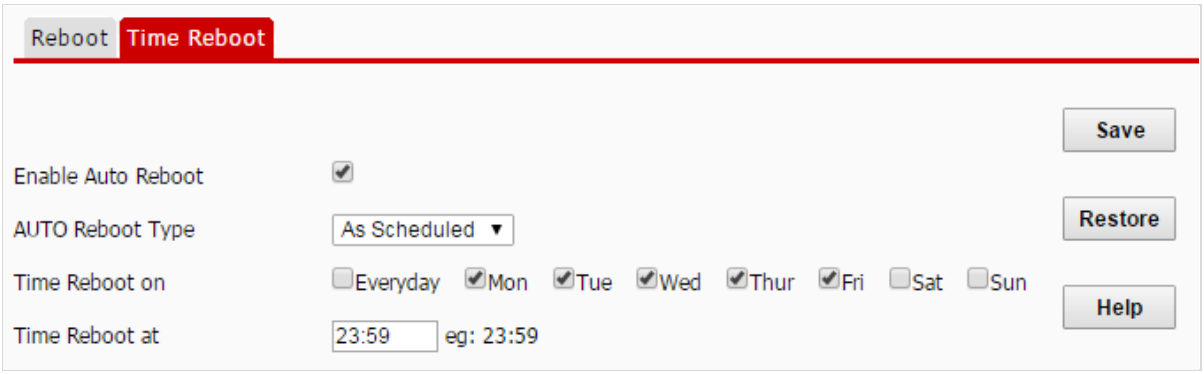
1. Check the **Enable Auto Reboot** box.

2. Select **As Scheduled** from the drop-down list.

3. Check corresponding dates from Mon (Monday) to Sun (Sunday) to specify the reboot date.

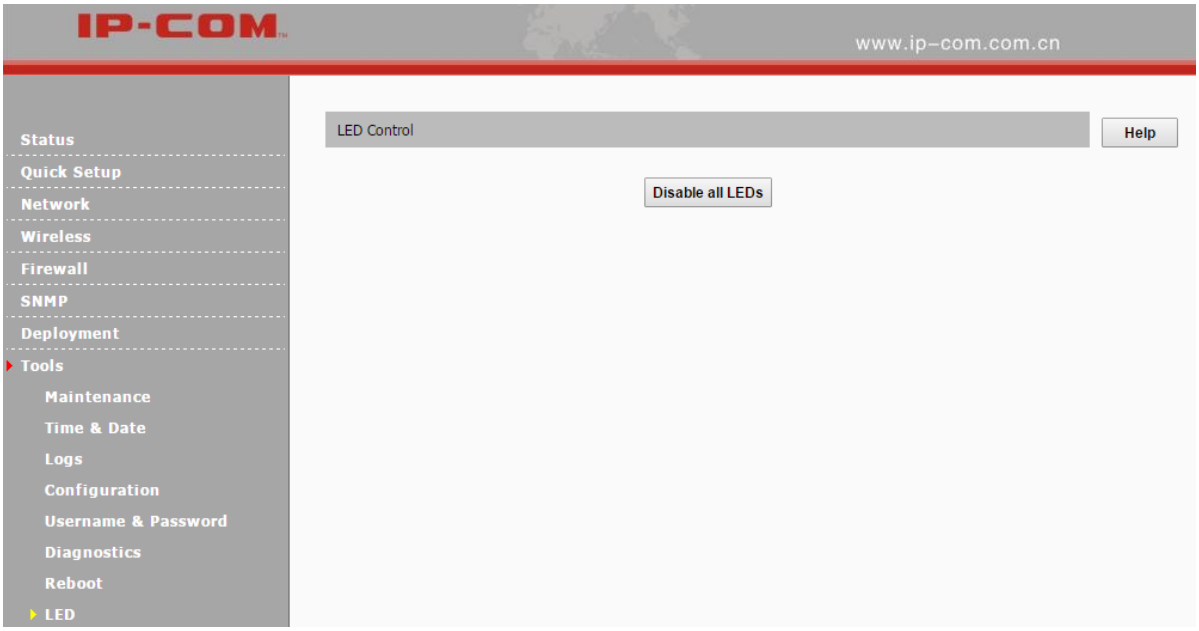
4. Specify the reboot time.

5. Click **Save** to apply your settings.



3.8.8 LED

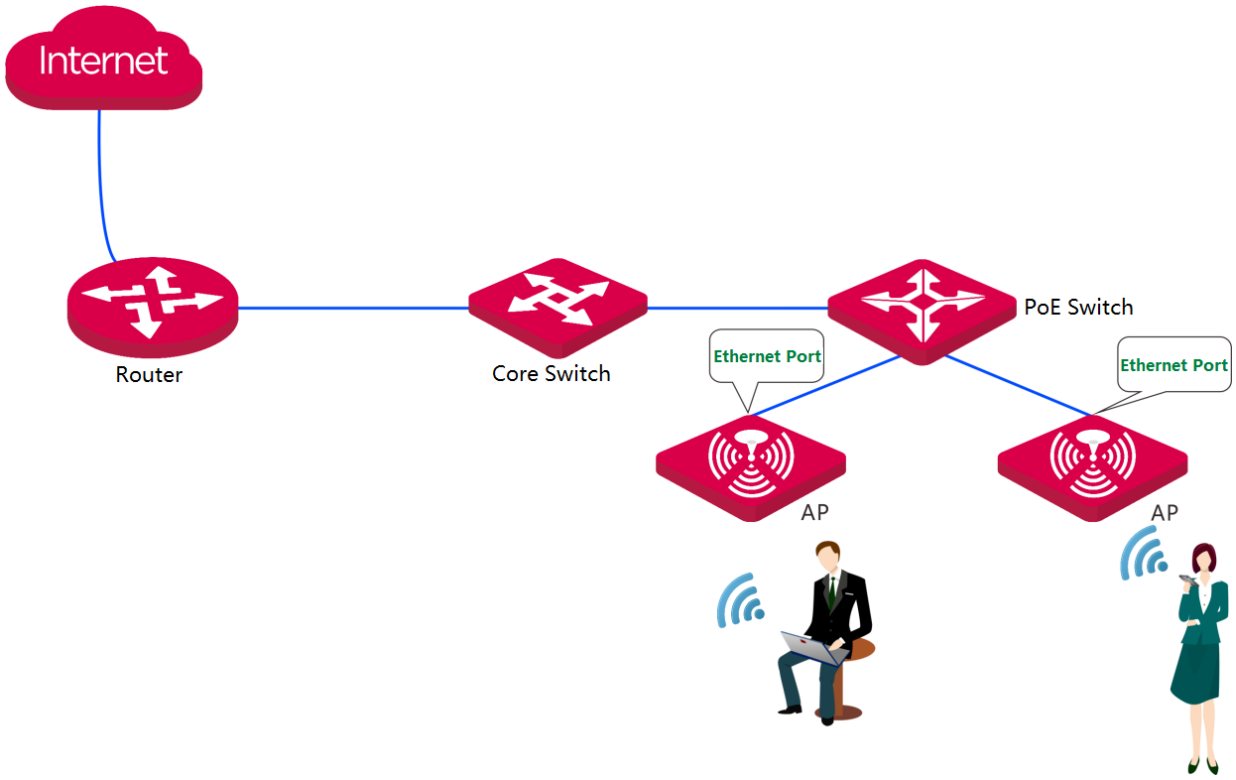
Click **Tools > LED** to turn off/on all LEDs.



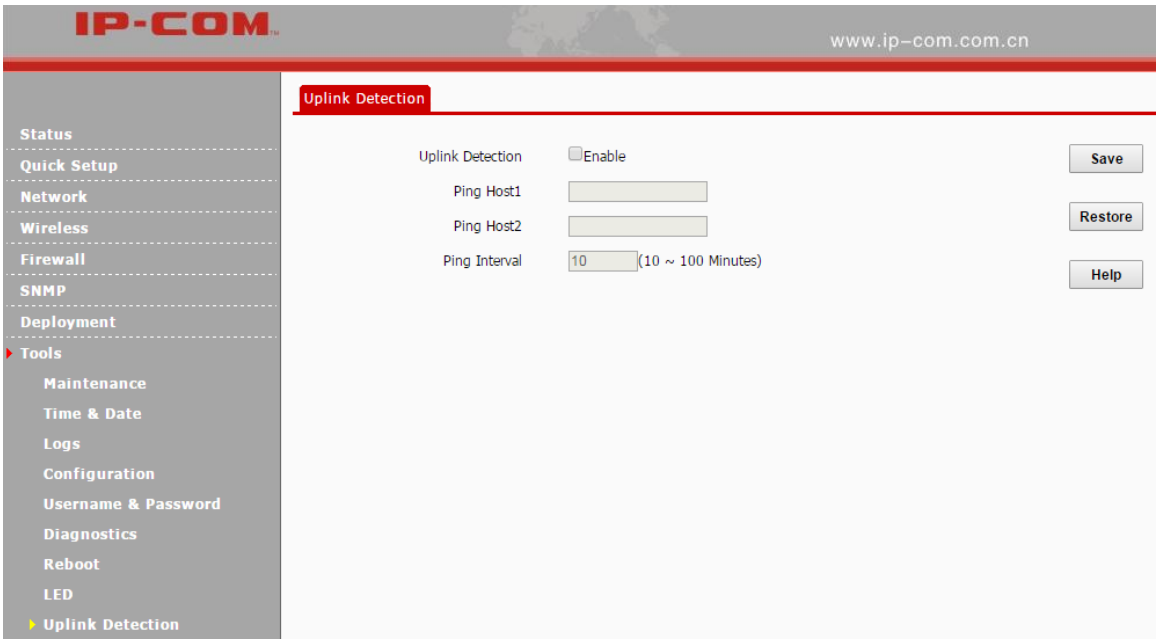
3.8.9 Uplink Detection

When "Uplink Detection" is enabled, AP will periodically Ping the configured host. If its Ping packets are unreachable to the host, wireless clients will re-associate with another AP by disabling this AP's SSID broadcast. This action can ensure that the client can connect to an AP which has normal access to the Internet.

The network topology is shown as below:



Click **Tools > Uplink Detection** to enter page below:



Parameters Description:

Item	Description
Uplink Detection	Enable/Disable the uplink detection feature.
Ping Host 1/2	Specify the address of the Ping host which connects to the Ethernet port of the AP.
Ping Interval	Configure the interval for Ping test.

4

Appendix

FAQs

Configure PC

Default Settings

Safety and Emission Statement

A FAQs

Q1: I enter 192.168.0.254 in the web browser but cannot access this AP's web UI. What should I do?

- Verify that Ethernet cables are properly connected;
- Check the TCP/IP settings on your PC and verify that IP address is 192.168.0.X (2-253);
- Clear the browser cache or try another web browser;
- Disable the firewall of your PC or try another PC;
- If there are at least 2 APs in your network, and they are not centrally managed by an AC, please connect APs one by one to the switch and modify their IP addresses.
- If your AP has been managed by an AC, its login IP address might not be 192.168.0.254. Log in to the AC, view the new IP address of your AP and then use the new one to log in to it.

If you are still unable to log in, please press the RESET button to restore the device to its factory default settings and follow this install guide to configure your settings again.

Q2: The AP can't be discovered by the AC. What should I do?

- Verify the AP has been connected properly and powered on.
- If VLAN has been divided in your network, verify that corresponding VLAN settings have been configured on the AC.
- Restart or reset your AP and try again.

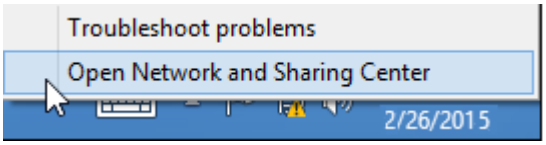
For more info, you can visit our website http://www.ip-com.com.cn, send an e-mail to info@ip-com.com.cn, or give us a call by (86755) 2765 3089. We'll help you out as soon as possible.

B Configure PC

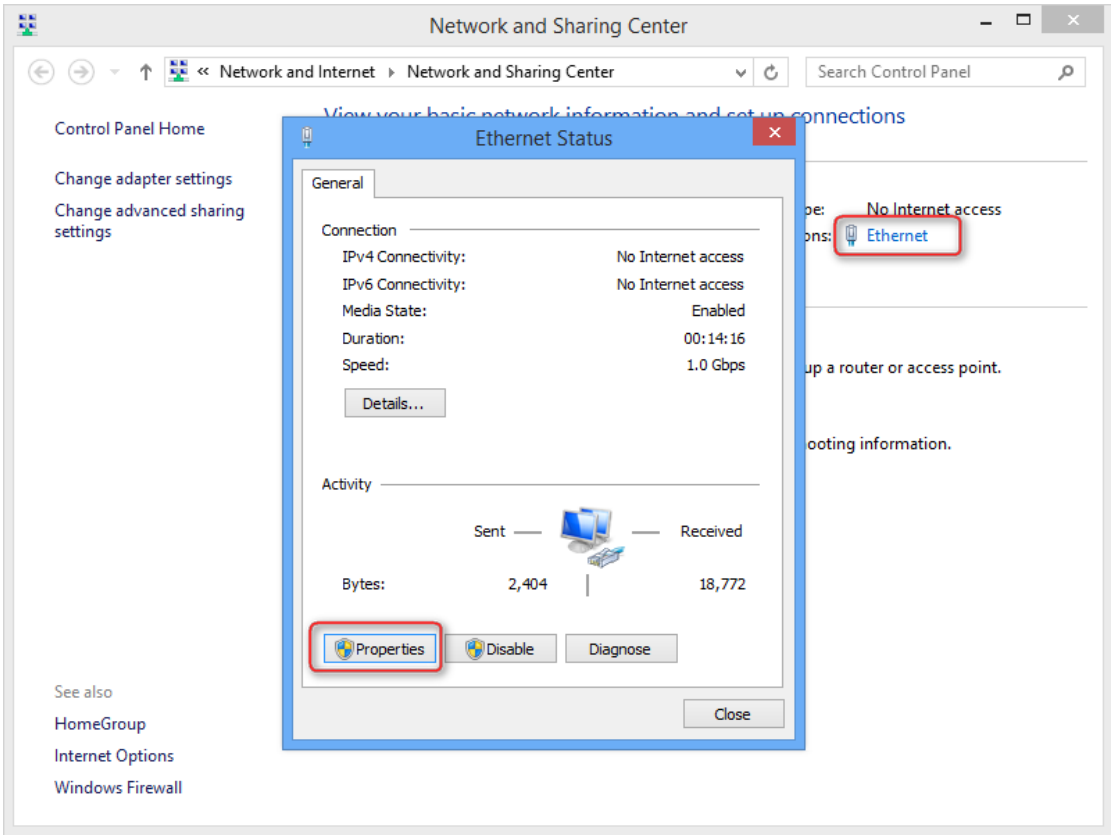
Windows 8

1. Right click the icon on the bottom right corner of your desktop.

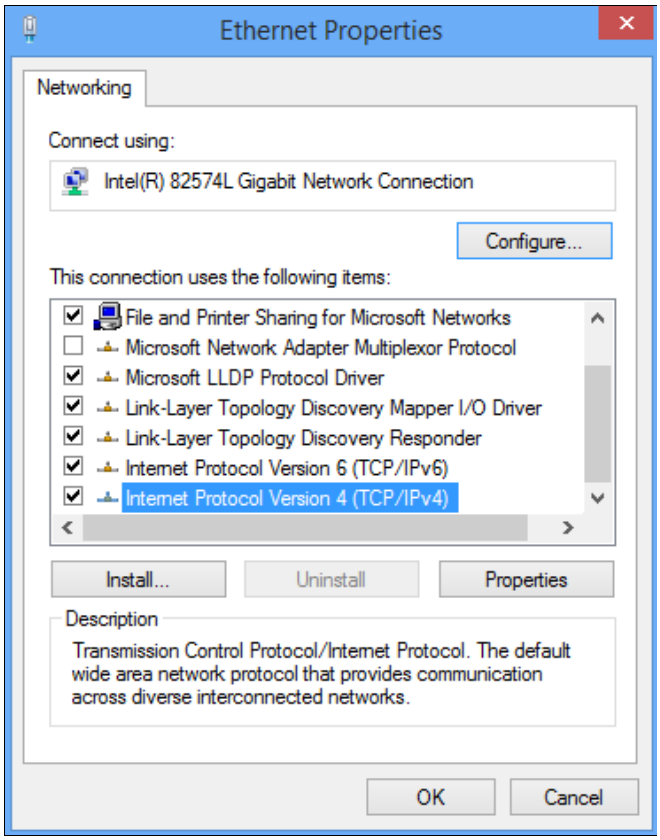
2. Click **Open Network and Sharing Center**.



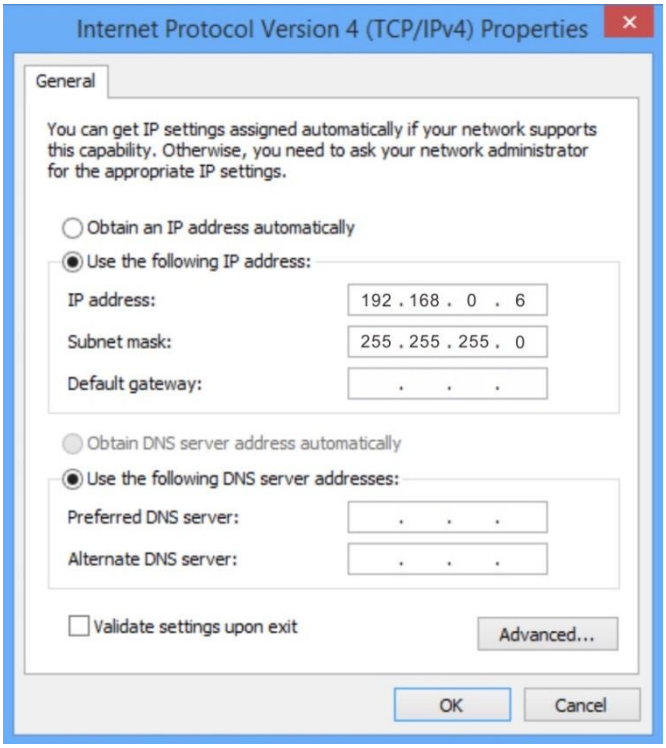
3. Click **Ethernet** > **Properties**.



4. Find and double click **Internet Protocol Version 4(TCP/IPv4)**.



5. Select **Use the following IP address**, type in the IP address: **192.168.0.x** (2~253), Subnet mask: **255.255.255.0** and click **OK**.

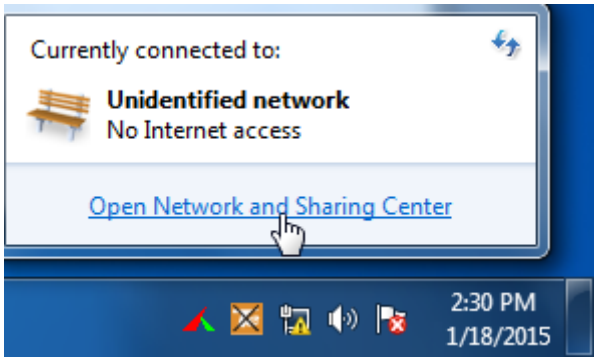


6. Click **OK** on the **Ethernet Properties** window.

Windows 7

1. Click the icon on the bottom right corner of your desktop.

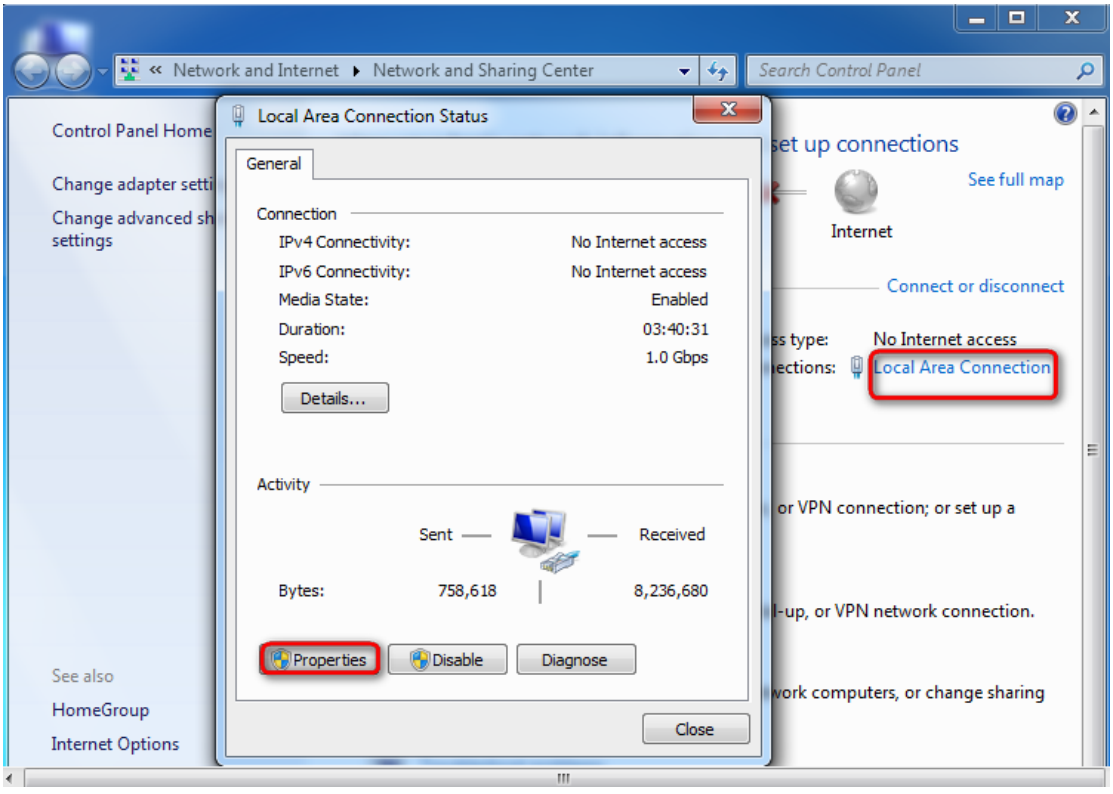
2. Click **Open Network and Sharing Center**.



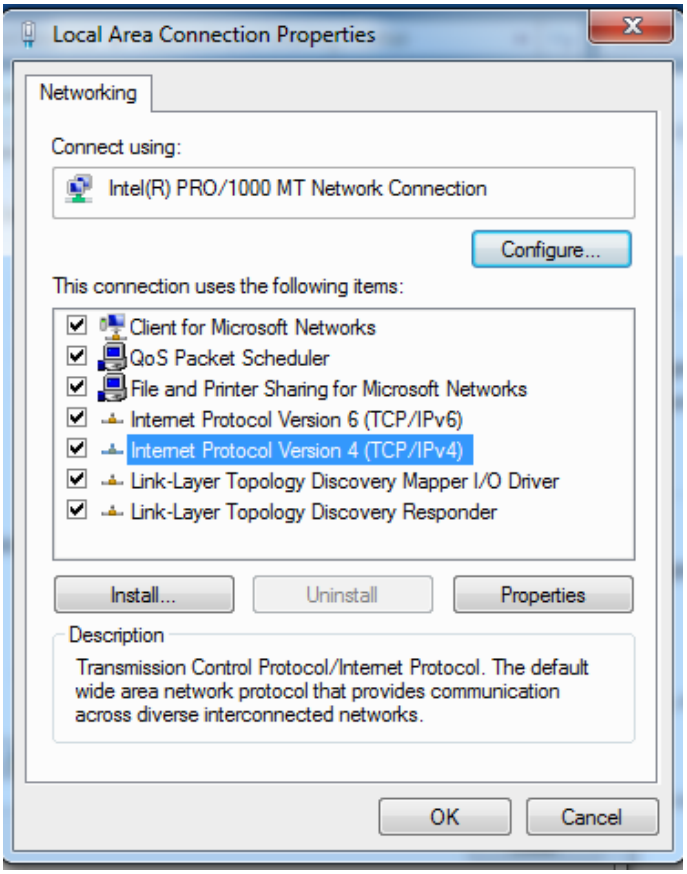
Tip

If you cannot find the icon on the bottom right corner of your desktop, follow steps below: Click **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

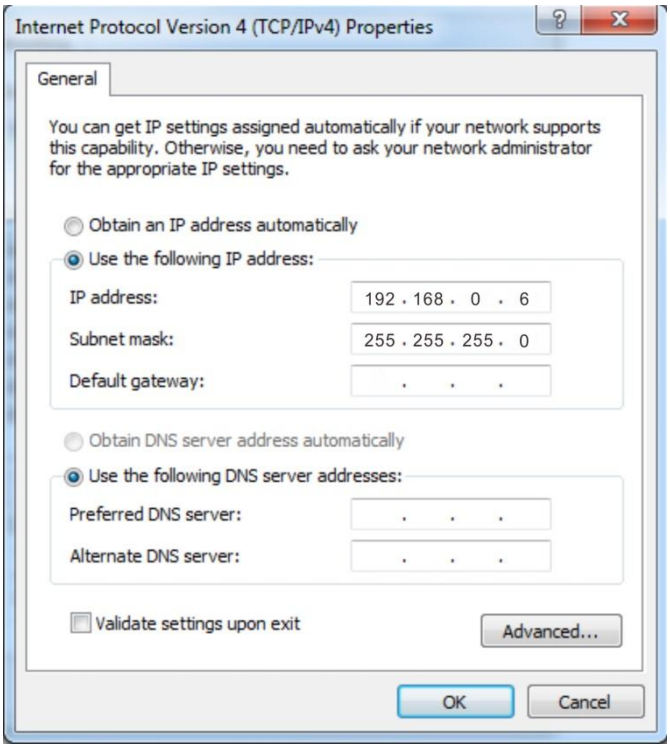
3. Click **Local Area Connection** > **Properties**.



4. Find and double click **Internet Protocol Version 4(TCP/IPv4)**.



5. Select **Use the following IP address**, type in the IP address: **192.168.0.x** (2~253), Subnet mask: **255.255.255.0** and click **OK**.

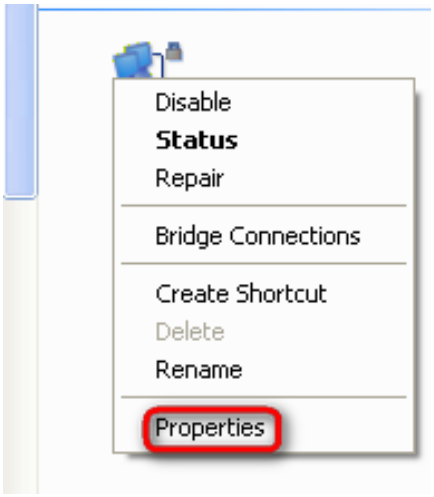


6. Click **OK** on the **Local Area Connection Properties** window.

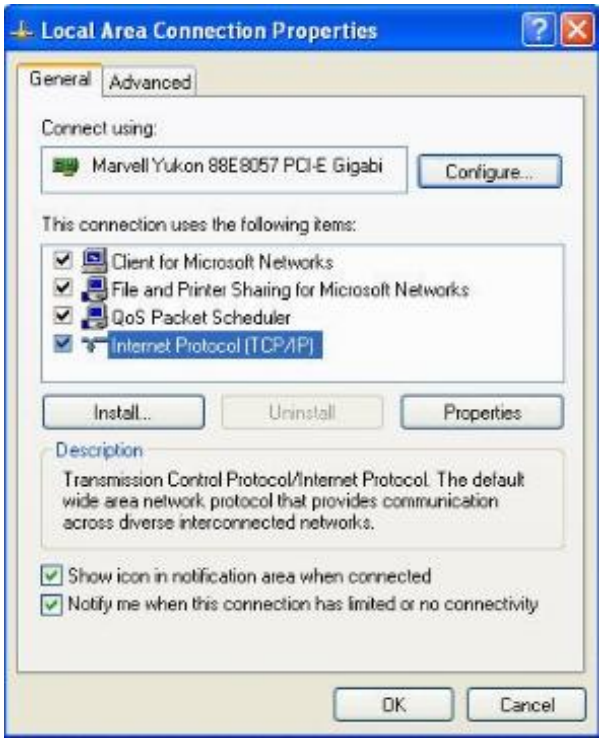
Windows XP

1. Right click **My Network Places** on your desktop and select **Properties**.

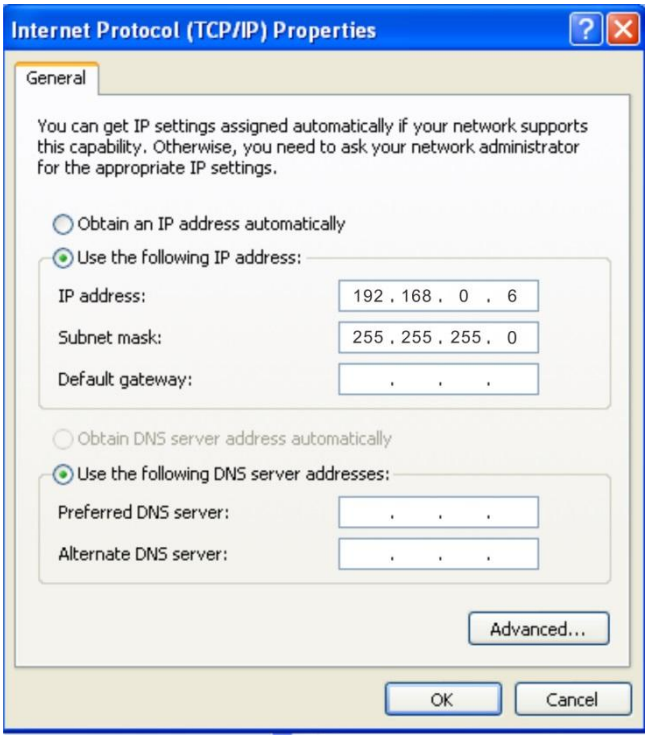
2. Right click **Local Area Connection** and select **Properties**.



3. Scroll down to find and double click **Internet Protocol (TCP/IP)**.



4. Select **Use the following IP address**, type in the IP address: **192.168.0.x** (2~253), Subnet mask: **255.255.255.0** and click **OK**.



5. Click **OK** on the **Local Area Connection Properties** window.

C Default Settings

Parameters			**Default Settings**
Device Login	IP		192.168.0.254
	User Name|Password	Administrator	admin|admin
		User	user|user
Quick Setup	Working Mode		AP mode
LAN sETUP	Address Mode		Static IP
	IP Address (Management IP)		192.168.0.254
	Subnet Mask		255.255.255.0
	Gateway		192.168.0.1
	Primary DNS server		192.168.0.1

	Secondary DNS Server		/
	Device Name		AP355
DHCP Server			Disable
SNMP			Disable
Deployment			Local
Tools	Time & Date	System Time	Sync with Internet time server. Time zone: (GMT+08:00)Beijing, Chongqing, Hong Kong, Urumuqi, Taipei
		Web Login Timeout	5 minutes
	Number of Logs		150
	Time Reboot		Disable
	LED		On

Parameters				Default Settings
Wireless	SSID Setup	SSID	2.4G Primary SSID	IP-COM_XXXXXX
			5G Primary SSID	IP-COM-5G_YYYYYY
		SSID	Primary SSID	Enable
			Other SSIDs	Disable
		Broadcast SSID		Enable
		Client Isolation		Disable
		Multicast to Unicast		Disable
		Probe Broadcast Packets Control		Disable
		Maximum Clients		48
		Chinese SSID Encode		UTF-8
		Security Mode		None
	Radio	WiFi		Enable
		Country		China
		Network Mode		2.4G: 11/b/g/n mixed; 5G: 11ac
		Channel		Auto
		Channel Bandwidth		2.4G: 20/40MHz; 5G: 80MHz
		Extension Channel		2.4G: Auto; 5G: /
		Channel Lockout		Disable
		TX Power		2.4G: 22dBm; 5G: 20dBm
		Power Lockout		Disable
		Preamble		Long Preamble
		Short GI		Auto
		Inter-SSID User Isolation		Disable

Parameters			Default Settings
Wireless (Continued)	Radio Optimizing	Beacon Interval	100
		Fragment Threshold	2346
		RTS Threshold	2347
		DTIM Interval	1
		Receive Signal strength	-90dBm
		Signal Transmission	Available for 2.4G, coverage-oriented
		5G SSID Priority	Available for 5G, disable
		Airtime Scheduling	Disable
		Interference mitigation	Available for 2.4G, 4
		APSD	Disable
		Ageing Time	5 minutes
		Basic Rate Sets	2.4G: 1, 2, 5.5, 11Mbps 5G: 6, 12, 24Mbps
		Supported Rate Sets	2.4G: 6, 9, 12, 18, 24, 36, 48, 54Mbps 5G: 9, 18, 36, 48, 54Mbps
	WMM Setup	Enable, Optimized for Throughput (concurrent users ≤ 10)	
	Access Control	Disable	
	Advanced	Recognize Terminal Type	Disable
		Filter Broadcast Data	Disable
	QVLAN	Disable	

D Safety and Emission Statement

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Operations in the 5.15-5.25GHz band are restricted to indoor use only.

This equipment complies with the European Council Recommendation of 12 July 1999 on the Limitation of Exposure of the General Public to Electromagnetic Fields [1999/519/EC].

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

This device is restricted to be used in the indoor.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

— Reorient or relocate the receiving antenna.

— Increase the separation between the equipment and receiver.

— Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

— Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement

This device complies with FCC radiation exposure limits set forth for an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.